1025 A-0 Y4.Sci2:99-58

FEDERAL GOVERNMENT COMPUTER SECURITY

513 Specials 25 MF/113 ORIGINAL

HEARINGS

BEFORE THE

SUBCOMMITTEE ON
TRANSPORTATION, AVIATION, AND MATERIALS

AND THE

SUBCOMMITTEE ON
SCIENCE, RESEARCH AND TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST SESSION

OCTOBER 29, 30, 1985

[No. 58]

Printed for the use of the
Committee on Science and Technology

COMPLETED 1986

U.S. GOVERNMENT PRINTING OFFICE
55-930 O WASHINGTON : 1986

I

BEST COPY AVAILABLE

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
TIMOTHY E. WIRTH, Colorado
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY, Florida **
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia
TERRY BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
BART GORDON, Tennessee
JAMES A. TRAFICANT, JR., Ohio

MANUEL LUJAN, JR., New Mexico *
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, JR., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID W. MORRISON, Washington
RON PACKARD, California
JAN MEYERS, Kansas
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
WILLIAM W. COBEY, JR., North Carolina
JOE BARTON, Texas
D. FRENCH SLAUGHTER, JR., Virginia
DAVID S. MONSON, Utah

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
REGINA A. DAVIS, *Chief Clerk*
JOYCE GROSS FREIWALD, *Republican Staff Director*

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

GEORGE E. BROWN, JR., California, *Chairman*

DAN GLICKMAN, Kansas
HARRY M. REID, Nevada
BILL NELSON, Florida
BART GORDON, Tennessee

TOM LEWIS, Florida
SHERWOOD L. BOEHLERT, New York
RON PACKARD, California

SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY

DOUG WALGREN, Pennsylvania, *Chairman*

STAN LUNDINE, New York
NORMAN Y. MINETA, California
GEORGE E. BROWN, JR., California
TIMOTHY E. WIRTH, Colorado
TERRY BRUCE, Illinois
TIM VALENTINE, North Carolina

SHERWOOD L. BOEHLERT, New York
DON RITTER, Pennsylvania
PAUL B. HENRY, Michigan
WILLIAM W. COBEY, JR., North Carolina

---

*Ranking Republican Member.
**Serving on Committee on the Budget for 99th Congress.

BEST COPY AVAILABLE

CONTENTS

WITNESSES

	Page
October 29, 1985:	
William S. Franklin, Associate Director, Information Management and Technology Division, U.S. General Accounting Office, accompanied by Raymond, J. Wyrsch, senior attorney, Office of the General Counsel, and Dr. Harold J. Podell, Group Director, Information Management and Technology Division	3
Richard P. Kusserow, Inspector General, Department of Health and Human Services, accompanied by John I. Molnar, senior analyst, and Vincent Mazzuca, Director, EDP Audit Division	58
Robert W. Beuley, Deputy Inspector General, U.S. Department of Agriculture, accompanied by Donn E. Adkisson, Assistant Inspector General for Audit	86
Robert E. Conley, president, Conley & Associates, Inc	100
October 30, 1985:	
James H. Burrows, director, Institute for Computer Sciences and Technology	115
Robert L. Brotzman, assistant director for Computer Security, Computer Security Center, National Security Agency	128
Donn B. Parker, senior management systems consultant, Information Systems Management Department, SRI International	151
William Franklin, Associate Director, Information Management and Technology Division, U.S. General Accounting Office, accompanied by Dr. Harold J. Podell, Group Director, Information Management and Technology Division, GAO and Raymond J. Wyrsch, senior attorney, Office of the General Counsel, GAO	164
Terry W. Culler, Associate Director, Workforce Effectiveness and Development, Office of Personnel Management	182

APPENDIX

Statement of Joseph R. Wright, Deputy Director, Office of Management and Budget	187

BEST COPY AVAILABLE

FEDERAL GOVERNMENT COMPUTER SECURITY

TUESDAY, OCTOBER 29, 1985

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE AND TECHNOLOGY, SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS,

Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2325, Rayburn House Office Building, Hon. Dan Glickman presiding.

Mr. GLICKMAN. Good morning. Today the subcommittee continues with its examination of computer and telecommunications security and privacy in Federal agencies. We began looking at this subject over 2 years ago. What we found at that time was extremely distressing. Computers and the communications links that connect them have become a vital tool of virtually every institution in our society. As a nation, we have become totally dependent on them.

Yet, despite their critical importance and the almost priceless value of much of the data stored within them, we have effectively ignored the threat imposed by improper use or unauthorized penetration.

The situation, I regret to say, is especially severe in Government. The data in Government computers is susceptible to manipulation, penetration, and unauthorized access. And what's worse, there is great confusion about who is in charge.

The Office of Management and Budget has statutory responsibility under the Paper Work Reduction Act. But as we have found in recent hearings, OMB has been, to say the least, timid in carrying out its responsibilities in the computer security area. Indicative of its hands-off attitude is the fact that OMB declined to testify today regarding the steps it is taking to implement the law.

In my opinion, that is most unfortunate, because OMB is probably in the best position of any agency to do something about a condition that is universally regarded as a problem, but OMB has chosen to be a nonplayer.

Meanwhile, the national security community, under the leadership of the National Security Agency, has initiated a well organized scheme for dealing with computer and communications security in the Federal Government. This plan, which is spelled out in National Security Decision Directive 145, creates an interagency committee to provide guidance and set standards for all Government agencies that handle both classified information and a new, but not well defined, category of sensitive information.

BEST COPY AVAILABLE

The overall concept is a good one. Clearly, someone needs to take charge, and NSA has stepped forward.

I do, however, have some reservations about the specifics of the directive. We found, for example, in hearings last summer that the military has a disproportionate influence in the standard-setting process—something that concerns many civil agencies. And there were several other defects that I won't recount here.

In our hearing today we plan to focus on the posture of computer and telecommunications in the Government. The centerpiece of this session is a year-long study done by the GAO, at this subcommittee's request, on the effect and status of computer security at a number of Federal agencies. In effect we have asked the GAO to render a report card on each of these agencies. Following GAO, we will hear from other witnesses, either currently in Government, or recently retired from it, about their view of problems in computer security.

Tomorrow we plan to turn to a consideration of solutions to these problems. At that time we will join with the Subcommittee on Science, Research and Technology to hear comments on H.R. 2889, which I introduced, the Computer Security Research in Training Act of 1985.

I might also mention that that bill was jointly referred to the Committee on Government Operations. The subcommittee on that committee, which has been chaired by Mr. Brooks of Texas, has reported out this bill with significant amendments to it dealing with the national security related issues. That bill is going to the full Government Operations Committee today, and 2889 may be reported out of Government Operations today. I suspect that the bill, in some form, will be reported out of this committee fairly soon. So, legislatively we intend to take action in this area.

Now I would like to yield to Mr. Lewis of Florida.

Mr. LEWIS. Thank you, Mr. Chairman.

Virtually every American citizen today is affected in some way by computers used by the Federal Government. Everything from keeping our tax records to managing the air traffic control system is handled by computer today. Yet, few Americans fully comprehend how vulnerable they are to misuse or outright criminal abuse of this technology.

This subcommittee has held a number of hearings over the past few years to learn more about this problem, and by doing so, has helped to increase public awareness of this issue. More people are becoming aware of the need for computer security and the consequences of unauthorized access to the data in those computers. Unfortunately, computer security has a cost associated with it, not the least of which is inconvenience to the user. User friendly is the feature most often sought by users of computers, and this is not generally compatible with security. It is clear that security has lagged behind other aspects of computer technology and much still needs to be done.

You are to be commended, the gentleman from Kansas, for your efforts in this area and for the work that you have done over the past several years, and also I commend the chairman for continuing these hearings.

BEST COPY AVAILABLE

The survey conducted by the General Accounting Office should be very helpful in assessing the status of computer security in Federal Government systems. I look forward to hearing the results of the survey.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you, Mr. Lewis.

Mr. Franklin, we appreciate your being here. I might mention that you have basically done your work in connection with the request made by this subcommittee. What you are giving us today is basically a survey results rather than a formal printed report which would have taken a significant additional period of time, as I understand it; is that correct?

Mr. FRANKLIN. That's correct.

Mr. GLICKMAN. I would say for the record, that's because we wanted to get an expedited or accelerated report not only on the current status of information but also on what is happening now and what will be happening in the future.

After we go through this material, we may want to talk to you further about whether we should go ahead and pursue some form of formal report or not, but at least at the current time you have complied with what the subcommittee has asked you to do.

We would ask you to present your testimony. The entire report will appear in the record, everything you have submitted to us. So you may summarize or proceed as you deem appropriate.

STATEMENT OF WILLIAM S. FRANKLIN, ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY RAYMOND J. WYRSCH, SENIOR ATTORNEY, OFFICE OF GENERAL COUNSEL, AND DR. HAROLD J. PODELL, GROUP DIRECTOR, INFORMATON MANAGEMENT AND TECHNOLOGY DIVISION

Mr. FRANKLIN. Thank you.

Mr. Chairman and members of the subcommittee:

We are pleased to be here today to discuss the status of computer and telecommunications security for selected automated information systems within Federal civil agencies.

I have with me Dr. Harold Podell, on my left, group director from our Information Management and Technology Division, and Mr. Ray Wyrsch, senior attorney from our Office of General Counsel, with me today on my right.

Mr. Chairman, as the Government becomes increasingly dependent on computers to do its work, automated information systems security takes on even greater importance than before. By using two questionnaires and through subsequent interviews, we surveyed the security status of 25 mission-critical automated information systems at 17 agencies.

Our survey involved systems that (one) make monthly payments to millions of beneficiaries of various Government programs; (two) process electronic funds transfers involving financial institutions; and (three) maintain online information essential to safeguarding human safety and the economic vitality of key U.S. industries.

We believe that good automated information systems security consists of two elements: first, management responsibilities and,

BEST COPY AVAILABLE

second, the establishment of actual security safeguards. Management responsibilities include such steps as prescribed in Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1, which requires agency heads to establish policies and procedures and assign responsibilities for automated information systems security. Actual security safeguards are those measures necessary, both in and around automated systems, to protect sensitive mission-critical data.

Generally, the results of our survey showed that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste. Specifically we found that:

Key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program; and the actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques, such as passwords, allowing access to systems were not always periodically changed.

As you can see in our first chart, no one management element was implemented by all of the 25 systems. Note also that training, ADP personnel security, assigned responsibility, and budgeting and accounting for security costs were implemented for only a few systems.

Mr. GLICKMAN. Could I ask you to stop for 1 second so we understand what we are looking at?

Mr. FRANKLIN. Yes.

Mr. GLICKMAN. You are looking at—when you say number of systems meeting requirements, are you talking about Federal agencies there?

Mr. FRANKLIN. We are talking about the specific automated information systems within the 17 agencies.

Mr. GLICKMAN. How many total systems would be subject to——

Mr. FRANKLIN. Twenty-five.

Mr. GLICKMAN. Twenty-five. So as we look through each one of these things—risk management, only 8 of the 25 systems met that requirement?

Mr. FRANKLIN. Met the criteria that we put forth for that element, right.

Two of these key management responsibilities, namely, automated information systems security training and risk management, deserve special mention.

Security training is important to ensure that agency personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of, and know how to meet, their security responsibilities.

The second management responsibility we would emphasize is risk management. The objective of this approach is to strike an economic balance between the expected loss associated with the risk and the cost of protective safeguards. The approach should include determinations of data sensitivity; second, system vulnerabilities, threats, and risks; third, alternative safeguards, their costs, and relative benefits; and, fourth, the most appropriate safeguards.

In looking at other management responsibilities, we also found weaknesses. For example, while contingency plans were developed for 18 systems, only 9 of them were tested. Failing to meet respon-

BEST COPY AVAILABLE

sibilities like this one can have an undesirable effect on the security of systems. For example, without developing and testing contingency plans, organized recoveries in the event of a major emergency are not assured.

Chart 2 (appendix v) shows examples of potential effects of missing management elements. If you will take a look at the chart, you will see the first one: Lack of Risk Management. A potential effect is that controls will be more than likely missing, or not cost effective. You don't know. If you don't undergo a risk management approach, including a comprehensive risk assessment, you are not assured that you can even identify the majority of your threats and vulnerabilities, and even know what your risks are, let alone the value associated with those risks—what your exposure is.

Such deficiencies are of particular concern because they can lead to weaknesses in the security safeguards, my next topic.

There are three categories of safeguards: physical, technical, and administrative. The necessary protection levels and combinations of safeguards should be identified in the risk management process. Although there is no such thing as absolute security, a balance of these three categories of safeguards is needed. Without such a balance, existing controls may be more easily circumvented. For example, without adequate separation of duties technical safeguards may be bypassed.

As you can see from chart 3 (appendix V), only five systems contain each of the physical, technical, and administrative safeguards evaluated.

Physical safeguards include measures, such as locks, badges, alarms, or similar devices. As the chart shows, only 16 out of 25 mission-critical systems were protected by physical perimeters, such as fences or detection devices.

Technical safeguards are automated system features that help control access, limit user privilege, maintain program and data integrity, and provide the needed tools for detecting security violations.

For criteria in assessing technical safeguards, we used selected provisions of the Department of Defense trusted computer systems evaluation criteria—to date the most comprehensive criteria for establishing technical safeguards. We used selected provisions that we believe are most appropriate for civil agency implementation.

One of the important technical safeguards is the capability of the system to identify and authenticate users. Twenty-three of the twenty-five systems contained this capability.

Another important technical safeguard is the maintenance of audit trails. Only 10 systems meet this criteria.

The final category shown on the chart involves administrative safeguards. These are nonautomated techniques for safeguarding information systems and include procedures, practices, separation of duties, and a broad range of other techniques.

Agencies have weaknesses in key administrative safeguards. One of the major threats to any automated information system is from inside the organization, namely, intentional and unintentional actions of employees. For instance, separation of duties is intended to prevent unauthorized actions by employees. We found that written procedures and/or organizational structures did not always provide

BEST COPY AVAILABLE

for separation of duties necessary for the execution of critical functions.

We also found instances where data processing security procedures were not tested to ensure that they were effective.

Chart 4 (appendix V) shows the potential effect of not having selected safeguards in place. For example, without audit trails there are limited means to track actions or security violations or to determine quickly the impact of unauthorized access to the system or agency.

In conclusion, no agency met all management responsibilities, and only five systems evaluated contained each of the safeguards studied. Improvements are needed in both of these important areas.

With regard to making these improvements, officials of several agencies cited reasons for the shortfalls in implementing management responsibilities and security safeguards. These included a lack of management commitment; funds and resources; and assistance in implementing policy and guidance.

Therefore, Mr. Chairman, these determinations lead us to conclude that the automated information systems studied are vulnerable to threats and their potential effects. It is the responsibility of agency heads to ensure that policy and guidance emanating from the responsible central agencies are implemented. Our survey indicates that such policy and guidance often are not implemented.

This completes my prepared remarks. We would be pleased to answer any questions that you may have.

Mr. GLICKMAN. Thank you very much, Mr. Franklin.

Those charts—do you have—are they located in the summary information that you have given us?

Mr. FRANKLIN. Right, the charts are appendix V of the statement.

Mr. GLICKMAN. OK.

I would like to just ask you some basic questions. One is, how did you select the agencies and the systems to be surveyed? You picked 25 computer systems in Government.

Mr. FRANKLIN. Right.

Mr. GLICKMAN. How did you pick those 25, and which agencies?

Mr. FRANKLIN. OK. Basically it started as a negotiation process with your own staff as to what agencies were of interest and what systems were of interest, and taking into account our knowledge at GAO of specific important programs and associated systems in agencies as a result of over 40 products that GAO has produced in the past—a combination of reports, testimony, and what have you. And we used all of that knowledge to judgmentally decide which systems would more than likely be a good sampling—not in the statistical sense, but judgement sense—good sampling of major mission-critical systems in some of your major civil agencies. It was judgment, basically.

Mr. GLICKMAN. And how did you devise the questions in the questionnaires that you sent out?

Mr. FRANKLIN. OK. We were fortunate along those lines. We went to the DOD Computer Security Center, and they had a set of evaluation criteria, at least for the technical aspects of our survey. And they provided us a lot of assistance in terms of deciding which

BEST COPY AVAILABLE

questions were appropriate for civil agencies, and they just provided a lot of help—and very cooperative.

And for the management questions we used a combination of our own knowledge—a lot of the people on the team and other individuals at GAO have extensive ADP knowledge along technical lines and management lines—and we used a combination of that too.

Mr. GLICKMAN. And how did you validate the questionnaire responses? Did you do any testing to determine the effectiveness of various security measures?

Mr. FRANKLIN. Yes, we pretested the questionnaire at two agencies. I believe the Federal Reserve was one, and the other one, I believe, was Small Business.

Dr. PODELL. And also we had one other whose name I don't remember right now.

Mr. FRANKLIN. OK. We essentially tested it at two agencies, two systems; got back the results and refined the questionnaire again with assistance from DOD.

Mr. GLICKMAN. And now in dealing with the agencies, one, were they cooperative? And, two, did you have to promise them confidentiality to get them to answer the questionnaire?

Mr. FRANKLIN. First, yes, they were cooperative. And, yes, we did promise confidentiality. One thing we did not want to do is to create a situation where we made their systems vulnerable, or I say, more susceptible to a potential adverse action than they ordinarily would be by exposing their specific vulnerabilities, you know, in a public forum.

We do have a lot of information. We have presented closed briefings to your staff on FAA and Federal Reserve, which did give specifics, but we did promise confidentiality to the agencies.

Mr. GLICKMAN. Well, I am not going to breach that. I am aware of some of the specific agencies right now. But I would tell you that the purpose of this report, as well as the legislation which we have, is to get these agencies to improve their existing systems.

Mr. FRANKLIN. Right.

Mr. GLICKMAN. And if in fact I don't—we don't see that happening in the next year or so—and also, I am aware that they have some follow-on systems coming on board, computer systems, which may even be more critical in terms of their security measures than existing systems.

Mr. FRANKLIN. I understand.

Mr. GLICKMAN. But those agencies ought to know that information would be released dealing with specific vulnerabilities. And—now, let me ask you this—first of all, I want to read a couple of things in your statement, reread it for the purpose of the record. You say, specifically we found that key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program. And the actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques such as passwords allowing access to systems were not always periodically changed. Generally, we found that agencies have not executed all the management responsibilities, most of which are prescribed in current OMB policy and supplemented by NBS, National Bureau of Standards, guidelines, and Office of Per-

BEST COPY AVAILABLE

sonnel Management instructions. As you can see in our first chart, no one management element was implemented for all of the 25 systems.

You know, it looks to me like, based on your report, we have severe defects in computer security in these systems. Is that a fair statement?

Mr. FRANKLIN. I think it is a fair statement. The key is no one really displayed a well balanced approach. It is not just the physical, technical, and administrative safeguards. It's also the management elements. And if you look at both of those in combination, it's really the weakest link that's the problem. No one really undergoes a risk management exercise in the true sense of the word. What most people do today is they interpret the language in OMB circular A-71, Transmittal Memorandum No. 1, which requires a risk analysis—they interpret that as, well, identify my threats and vulnerabilities, and I make a judgement call as to what my risks are, then I postulate alternatives and I go through an exercise to cost out the safeguards associated with those alternatives.

The missing part is assigning an economic value to your risk. Once you determine your threats and vulnerabilities, you have an exposure. In most instances, you can assign a value, a dollar value, to that expected loss.

Mr. GLICKMAN. In most instances, you say you can assign?

Mr. FRANKLIN. In most instances, you can.

Mr. GLICKMAN. Well, let's say if the Federal Reserve System is one of the computers we are looking at, they have a dollar value of—of probably extraordinarily high potentiality in terms of a loss in the event that the information in their computers is—is either fraudulently or negligently misused. And that ought to be factored in in terms of determining what the cost of a—and the burden of a risk assessment would be?

Mr. FRANKLIN. In a general sense, yes, they ought to take cost into account, yes.

Mr. GLICKMAN. I just—going back, then, in terms of what problems do agencies have in doing risk assessments, did you find any overall guidance on the part of OMB, or anybody else, with respect to the agencies themselves doing risk assessments? Was OMB pushing agencies to doing risk assessments at all?

Mr. FRANKLIN. Not that we could identify. Let me turn you over to Dr. Podell. He personally had the interviews with OMB, maybe he can shed a little more insight into that.

Mr. GLICKMAN. OK, sure.

Dr. PODELL. Thank you.

We met with officials from OMB. They do have in their A-71 TM-1 an overall guidance requirement for this area but the available guidance, which is National Bureau of Standards, Federal Information Processing Standard, No. 65, is really not, in my opinion, enough guidance, enough specificity to the agencies. And that's part of the dilemma we found in working with these agencies and these 25 systems.

Mr. GLICKMAN. And then, therefore, each agency and/or each system is basically going its own way with respect to risk assessment, then; is that a fair statement?

BEST COPY AVAILABLE

Dr. PODELL. That is a fair statement. We found that the agencies do what they feel is best given the available state of the guidance on risk management.

Mr. GLICKMAN. Now, on a scale of 1 to 10—this is a difficult question but I would ask you inasmuch as you work for us—on a scale of 1 to 10, how would you rate the overall security of the 25 Federal systems you surveyed relative to full compliance with existing guidance and good practice?

Mr. FRANKLIN. OK. First let me qualify my answer before I give it.

There's a lot behind these figures. For any one of those categories there may be half a dozen to a dozen elements that make them up in terms of specificity. Now, the data that we cannot present because it relates to specific systems would give a more clear understanding of the basis for my answer.

Basically, I would have to say I would put them somewhere in the category of 5 to 6 overall. These are just the 25 that we evaluated on that scale of 1 to 10—somewhere in the range of 5 to 6.

Mr. GLICKMAN. They clearly have a long way to go, then.

Mr. FRANKLIN. They have quite a ways to go, yes.

Mr. GLICKMAN. Yeah. And then in trying to refine that question a little further, can you, the GAO, tell the committee just how vulnerable these systems are?

Mr. FRANKLIN. They are very vulnerable in general. Basically because of what I mentioned before and what we have in the testimony as the lack of balanced approach; it's not only sufficient to have your technical safeguards in place. For example, you can go out and buy a secure package or a top secret package and overlay your operating system all you want. If you don't have the administrative apparatus in place to ensure that your passwords are changed, or that your user ID's are changed, or that when people leave passwords are purged, that type of thing, then you leave yourself open. And that's the weak link proposition. And that's basically the reason why a lot of these systems are highly vulnerable; because there are one or more missing elements from one of those categories: Your management, physical, technical, or administrative safeguards.

Mr. GLICKMAN. The bottom line is that only 5 systems out of 25, or 20 percent, have all the safeguards that you think that require to the physical, technical, and administrative safeguards to protect the systems and the information contained therein?

Mr. FRANKLIN. Right, and even that's only a portion of it, because that's physical, technical, and administrative safeguards. That doesn't address the management part.

Mr. GLICKMAN. For example, only two systems there are manage—one of the management responsibilities is training, only two systems have adequate training?

Mr. FRANKLIN. Right.

Mr. GLICKMAN. You say eight systems risk management and then you go down ADP personnel security, budgeting, and given all those things. So even though 5 out of 25 have all the administrative safeguards, even among those there might not be adequate training going on——

Mr. FRANKLIN. That's right.

BEST COPY AVAILABLE

Mr. GLICKMAN [continuing]. In those respective systems.

Do you have any idea the extent of financial losses incurred by the Government because of weaknesses in automated information systems security?

Mr. FRANKLIN. We didn't do that as part of this audit but in the past GAO has done an audit of benefit payment systems. And they did five benefit programs and came up with an aggregate value that approached $1 billion. Also, we are——

Mr. GLICKMAN. Benefit like so—you are talking about like——

Mr. FRANKLIN. Like computer matching done at SSA—that kind of thing.

Mr. GLICKMAN. Yeah, OK. Good security.

Mr. FRANKLIN. Yes, it's that kind of thing.

Another product we have is the American Bar Association report which—I don't know how technical it was or how structured it was in terms of actually verifying the value they came up with, but they came up with a value of about $50 billion.[1] But that's for all systems U.S. wide, Government and industry. And I think they got that as a result of a subjective judgment on the part of managers of major firms and major systems, and that kind of thing.

Mr. GLICKMAN. OK. Well, I would—I need more time to review the report that you have presented because today is the first day that I have actually seen it in depth. And after doing that the committee may have more questions for you. But I think it's a fair statement that your report reinforces—in fact, it enhances—the concern of this committee and others in Congress for the last 2 years, that Federal computer systems are in danger of being improperly used, negligently used, or otherwise. And the information contained therein is not as protected as the people in this country think it is.

Mr. FRANKLIN. I think you are absolutely correct.

Mr. GLICKMAN. Thank you.

Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman.

Mr. Franklin, with—was there any reasons given by the other agencies as to why they didn't meet the adequate training requirements for security?

Mr. FRANKLIN. Let me give you a general answer and then I will turn it over to Dr. Podell.

A general answer they gave to most any question regarding a lacking on their part was stated in the conclusion remarks that I made—basically, lack of management commitment, lack of funds and resources, lack of assistance and implementing policy and guidance.

Now, in terms of more specificity, let me turn it over to Dr. Podell who may have a little more insight.

Mr. LEWIS. Before we do that, they also use those reasons for the other inadequacies as well?

Mr. FRANKLIN. Yes.

Mr. LEWIS. Dr. Podell.

---

[1] Mr. Franklin meant to say, the equivalent or approximately $3 billion on a nationwide basis, although the actual nationwide losses could be much higher.

BEST COPY AVAILABLE

Dr. PODELL. Yes. As some examples of agency officials that we met with would amplify on what Mr. Franklin has pointed out, plus the fact in several cases the concept of training for computer security as related to the successful performance of agency mission is a relatively new concept. We had met with agency officials that couldn't relate the performance of their mission in a successful manner with the requirement for data integrity and other aspects of computer security. And I think that is an education problem for the managers themselves. So that's another example for the need to communicate to senior managers the importance of this type of training.

Mr. LEWIS. Do either one of you gentlemen feel we need additional legislation to try to correct this problem, be more specific? Maybe we need legislation that's going to say that a particular portion of any expenditure for these systems would include necessary funding, a percentage of funding for security and meeting those other deficiencies?

I would hate for us to go that far in legislation but apparently the way things seem to roll around here that's what it takes.

Mr. FRANKLIN. I think what you do need is legislation. But maybe not so much along the lines of providing funding, but more along the lines of assigning somebody the responsibility and authority to act as a central focus and act as the catalyst for this area. That's what's lacking—nobody's really acting as the catalyst. And I think on several occasions—one recently—DOD is trying to take on that role as acting as a catalyst, but that's one alternative. There are other aiternatives. But somebody has to do that. Somebody's got to push it.

Mr. LEWIS. You stated you used Governmentwide criteria which included OMB policy and NBS standards, OPM instructions, and DOD's trusted computer system evaluation criteria. Would you briefly tell us what these consisted of and were there any overlaps?

Mr. FRANKLIN. OK. The DOD computer systems evaluation criteria is basically a technical document, basically gets at the types of controls needed for various levels of assurance in the system. In other words, they tag things, for example, C–1 level, B–1 level, that type of thing, where you could get progressively more safeguards. And quite naturally it would cost more as you get progressively more safeguards. But the orientation is basically a technical orientation. It is basically on the features that are resident in your hardware architecture, the features that are resident in your system software like your operating systems, features required in any kind of supplementing support software like an overlay security package. Maybe you would have, say, if you have an IBM system, MVS operating system, and then you put on the top secret package that enhances the amount of features available to you to enhance the technical level of security in your system.

It does not go into a lot of the management elements or administrative procedures necessary.

I think a balanced approach between some of the good aspects of that technical document and some of the information presently in National Bureau of Standards guidelines is really what is needed for the civil agencies so that they can take into account all of the elements that they are required to, really. Right now, they aren't

BEST COPY AVAILABLE

required to because the guidelines are optional. The only thing they are required to do is make a subjective judgment on their own without criteria as to what they actually need. And that's where the hole is. That criteria needs to be brought together, needs to be brought together in a manner where it is put forth to the agency as an option they must consider.

So, there's a lot of room for joint guidelines, I think. I think the Bureau of Standards and DOD can really support one another in terms of putting out standards and guidelines and coordinating tightly so that they complement one another.

Mr. LEWIS. Thank you, Mr. Chairman.

Mr. GLICKMAN. I would just like to make two comments. One is I compliment GAO on the excellent job they did on this survey. I understand you had a large team working on this for about a year. I think this is very important. And this is one of the examples where legislative action comes from the kind of work that you are doing to indicate where a problem is. And this is not one of these pieces of legislation that any interest groups are fighting for. This is one of these things that we are working to try to protect people's interest who have information stored in computers, as well as protecting the Government's interest in keeping these computers secure.

I would like to also point out that, based upon what your charts have shown and the information you have provided us, as a general proposition agencies have done a better job at what you called the physical, technical, and administrative safeguards, which are basically more like the hardware items, you know: physical perimeters, uses of badge. The physical safeguards are the easiest ones to do because it is kind of a natural to protect the actual piece of equipment itself. Not quite as well on the technical safeguards, including the audit trail issue. And then the administrative safeguards have done—I don't know how you would categorize it with 25 being a perfect score. But when you look at the management items, the management evaluation of how computer security training is done and how computer security is treated as a separate element within a government's budget, and written procedures, and evaluations, and the kinds of things you actually have to do to protect the systems, it looks to me like these agencies have failed miserably in their attempt to protect the information.

And that looks like where the focus of both administrative and/or legislative action ought to take place.

Mr. FRANKLIN. I agree with you. That's correct, yes.

Mr. GLICKMAN. OK, we thank you for—oh, I'm sorry, Mr. Boehlert. I didn't mean to ignore you.

Mr. BOEHLERT. Thank you, Mr. Chairman. You're so enthused about the subject.

I would agree with your analysis, if I may follow up on what you just said, because it seems to me that the key element here is the lack of management commitment, as you point out on page 7 of your testimony. I am curious, Mr. Franklin, what level in the management structure did your survey carry you to? How high up did you go in the various departments and agencies you surveyed?

Mr. FRANKLIN. All levels. Basically, we went basically to the head of the systems area, which is at different levels in different agencies. In some cases that would take you to maybe the second or

BEST COPY AVAILABLE

third tier in the agency, because in some instances you may have, say, a commissioner and then you have a deputy commissioner that oversees the system area. And there may be several associate commissioners under him. So, in some cases it's the second or third tier. In other cases, because of the particular organizational structure of that agency, it may be a little further down.

We went to that level. And we also went out on the data center floors in selective followup. We couldn't do a complete followup across all the sites we went to, but we did do some selective followup where we actually went out on the data center floor to actually observe some of the things that were reported in the questionnaire. We didn't do any testing. We didn't really have the time to do that kind of thing. That is very intensive activity.

Mr. BOEHLERT. Were you welcomed?

Mr. FRANKLIN. In most instances yes, because we had already made the commitment to not disclose information about the specific systems, that the information would be presented in the aggregate. And their vulnerabilities would essentially be anonymous. So, once that was known, we got a lot of cooperation.

Mr. BOEHLERT. Did you have the feeling that the people you were talking with and you were surveying recognized that they have a serious security problem and really wanted to be part of the solution rather than just taking a ho-hum attitude about it?

Mr. FRANKLIN. From the contact I had, in most instances the working level does want to solve the problem. Now——

Mr. BOEHLERT. The working level. How about the management level? Does the management level recognize that a problem exists, do you feel, in most instances?

Mr. FRANKLIN. To a large extent the management level is not into specifics, so they really don't have a real good feel for the severity of the problem, which gets at the training again. You know, it's lack of exposure, whereas at the working level they're in it day in and day out. Now, as far as the central agencies, I don't have a firsthand feel for that. I will let Dr. Podell go into that in terms of what he sees as their commitment. By central, I mean GSA, OPM, and OMB.

Dr. PODELL. I would just like to give one example. We met with OMB officials, and we asked them what is the OMB commitment for providing policy and guidance in this area. It's essentially less than the equivalent of one full-time person for the entire area that we are talking about this morning.

Mr. BOEHLERT. That underscores your testimony then, the lack of commitment.

Thank you very much.

Mr. GLICKMAN. I would just like to make the point that you have in your testimony in the appendix listed under each category of safeguard the type of safeguard and the potential effect if the safeguard is not in place. So, I think from the standpoint of this committee and anybody else who is interested in reading, there is—you don't go into great detail about what could happen to the country if this doesn't happen, but I think you indicate physically what could happen, what loss of information is available, what lack of protection is actually available if the safeguard is not in place.

BEST COPY AVAILABLE

For example, you talk about, if audit trails are not reviewed, there's no reason to have an audit trail, and you can't trace the lack of information. You can't determine if the computer is providing any reasonable information at all. You talk about not having a security procedures manual. Some employees, new hires may be unfamiliar with controls and violate them. You talk about not purging system accounts, you know, the whole kinds of things that could happen to each system if it's not in place.

And I don't think you did any independent investigation at each agency, if these had in fact been violated, had you?

Mr. FRANKLIN. Right, we didn't go into that. That would have been testing.

Mr. GLICKMAN. Yes, you're talking more in the abstract about not having an audit system at all, you know. Plus, you talk about the variety of physical things, what the effect would be of not having them. And I think this is important in terms of at least in the abstract, trying to set the record for what can happen to our government computers and the information contained therein unless we get improvements in the operations of the systems and particularly relating to securing those systems.

Mr. FRANKLIN. We did run the potential effects in this appendix by the people at the National Bureau of Standards and DOD to verify that these were true potential effects if that situation existed. So, each of these have to some extent been confirmed by other experts.

Mr. GLICKMAN. But then to take a, so to speak, worst-case scenario, specifically, one would have to then follow on with, you know, theoretically you could determine if in fact, for example, somebody got into the air traffic control system or the system wasn't being operated correctly and we're missing some of these things, what theoretically could happen. Somebody else would have to do that follow on. You say you didn't do any of that kind of testing.

Mr. FRANKLIN. That's right. We didn't do any testing.

Mr. GLICKMAN. OK.

We thank you for your excellent work. We will be in further contact with you.

Mr. FRANKLIN. OK. Thank you.

[The prepared statement of Mr. Franklin follows:]

BEST COPY AVAILABLE

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 AM, EST
TUESDAY, OCTOBER 29, 1985

STATEMENT OF

WILLIAM S. FRANKLIN

ASSOCIATE DIRECTOR

INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

AUTOMATED INFORMATION SYSTEMS SECURITY

IN FEDERAL CIVIL AGENCIES

BEST COPY AVAILABLE

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the status of computer and telecommunications security for selected automated information systems within federal civil agencies. I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of General Counsel.

Mr. Chairman, as the government becomes increasingly dependent on computers to do its work, automated information systems security takes on even greater importance than before. By using two questionnaires and through subsequent interviews, we surveyed the security status of 25 mission-critical[1] automated information systems at 17 civil agencies.[2] Our survey involved systems that (1) make monthly payments to millions of beneficiaries of various government programs, (2) process electronic funds transfers involving financial institutions, or (3) maintain on-line information essential to safeguarding human safety and the economic vitality of key United States industries. Effective security in these systems is needed to prevent undesirable events, such as denial of benefits to citizens, unauthorized disclosure of sensitive information, loss of government money, waste of federal resources, human injury, and in extreme cases, loss of life and endangerment of the national welfare.

---

[1]Mission-critical systems are defined as those systems that significantly affect agency programs, finances, property, and other resources.

[2]For further details on our objectives, scope, and methodology, see appendix I.

BEST COPY AVAILABLE

We believe that good automated information systems security consists of two elements: management responsibilities and the establishment of actual security safeguards. Management responsibilities include such steps as those prescribed in Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, which requires agency heads to establish policies and procedures and assign responsibilities for automated information systems security. Actual security safeguards are those measures necessary, both in and around automated systems, to protect sensitive mission-critical data. As agreed to by experts, weaknesses in actual security safeguards increase system vulnerabilities and are often attributable to a lack of implementation of management responsibilities.

Generally, the results of our survey showed that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste. Specifically we found that,

--key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program, and

--the actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques (passwords) allowing access to systems were not always periodically changed.

In determining the status of agency automated information systems security, we primarily used the results of the questionnaires, interviews, and existing governmentwide criteria, which included

BEST COPY AVAILABLE

OMB policy, the National Bureau of Standards' (NBS') Federal Information Processing Standards (FIPS), Office of Personnel Management (OPM) instructions, and expert opinion. We also used the Department of Defense's (DOD's) Trusted Computer Systems Evaluation Criteria, which is being considered for future application by civil agencies. Detailed questionnaire results and potential effects of security problems are presented in the appendices to my statement.

I will now discuss in some detail the status of automated information systems security.

AGENCY SECURITY MANAGEMENT NEEDS IMPROVEMENT

Generally, we found that agencies have not executed all the management responsibilities, most of which are prescribed in current OMB policy and supplemented by NBS guidelines and OPM instructions. These management responsibilities are: risk management, training, assigned responsibility, budgeting and accounting for security costs, automatic data processing (ADP) personnel security, contingency plans, independent audit and evaluation, and written procedures. All of these responsibilities must be implemented in order to establish an effective combination of security safeguards. For example, ADP personnel security is needed to adequately protect the system from undesirable employee actions.

As you can see in our first chart, no one management element was implemented for all of the 25 systems. Note also that training, ADP personnel security, assigned responsibility, and

BEST COPY AVAILABLE

budgeting and accounting for security costs were implemented for only a few systems. Two of these key management responsibilities, namely, automated information systems security training and risk management, deserve special mention.

Security training is important to ensure that agency personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of and know how to meet their security responsibilities. This point was recognized in your Subcommittee's April 1984 report[3] on computer and communications security and privacy, which recommended that expanded training for all employees associated with automated information systems is needed so that they understand their roles for protecting sensitive data. While most agencies have some security training policies and/or procedures, only two have made efforts to formalize their approach by identifying, for example, audiences, course subjects needed, frequency of training, etc. Without a formalized approach, agencies cannot provide the necessary foundation for improving the security of automated information systems.

The second management responsibility we would emphasize is risk management. The objective of this approach is to strike an economic balance between the expected loss associated with the risk and the cost of protective safeguards. The approach should include

---

[3]Computer and Communications Security and Privacy. (Report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, dated Apr. 1984.)

BEST COPY AVAILABLE

determinations of (1) data sensitivity; (2) system vulnerabilities, threats, and risks; (3) alternative safeguards, their costs, and relative benefits; and (4) the most appropriate safeguards. Otherwise, agencies have less assurance that they are properly protecting the automated information systems effectively and economically. Risk management was applied to only eight of the systems studied.

In looking at the other management responsibilities, we also found weaknesses. For example, while contingency plans were developed for 18 systems, only 9 of them were tested. Failing to meet responsibilities like this one can have an undesirable effect on the security of systems. For example, without developing and testing contingency plans, organized recoveries in the event of a major emergency are not assured.

Chart 2 shows examples of potential effects of missing management elements. Such deficiencies are of particular concern because they can lead to weaknesses in the security safeguards, my next topic.

USE OF PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SAFEGUARDS NEEDS IMPROVEMENT

There are three categories of safeguards: physical, technical and administrative. These are established in OMB Circular A-71, Transmittal Memorandum No. 1. The necessary protection levels and combinations of safeguards should be identified in the risk management process. Although there is no such thing as absolute security, a balance of these three categories of safeguards is needed.

BEST COPY AVAILABLE

Without such a balance, existing controls may be more easily circumvented. For example, without adequate separation of duties technical safeguards may be bypassed.

As you can see from chart 3, only five systems contained each of the physical, technical, and administrative safeguards evaluated. I would now like to briefly discuss each of the three categories of safeguards.

Physical safeguards include measures, such as locks, badges, alarms, or similar devices, to protect personnel and property from damage by accident, fire, loss of utilities, environmental hazards, and unauthorized access. This category does not have as severe problems as other categories. However, as the chart shows, only 16 out of 25 mission-critical systems were protected by physical perimeters, such as fences or detection devices, outside the computer facility. Although agencies have taken steps to implement many of the physical safeguards, one might reasonably expect a computer center processing mission-critical systems to have some form of each of these.

Technical safeguards are automated system features that help control access, limit user privilege, maintain program and data integrity, and provide the needed tools for detecting security violations. For criteria in assessing technical safeguards, we used selected provisions of the DOD Trusted Computer Systems Evaluation Criteria--to date the most comprehensive criteria for establishing technical safeguards. We used selected provisions that we believe are most appropriate for civil agency implementation.

BEST COPY AVAILABLE

One of the important technical safeguards is the capability of the system to identify and authenticate users. Mechanisms such as passwords and user identification are generally accepted techniques to accomplish this objective. It is necessary that these mechanisms be protected by the system so their identity cannot be compromised. Twenty-three of the 25 systems contained this capability.

Another important technical safeguard is the maintenance of audit trails. An audit trail is a record that collectively provides documentary evidence of processing and should disclose (1) all attempted or actual accesses to the systems, programs, or files; (2) deletion or modifications of files; and (3) all system activity initiated by computer operators, system administrators, and/or system security officers. Only 10 systems meet these criteria.

The final category shown on the chart involves administrative safeguards. These are non-automated techniques for safeguarding information systems and include procedures, practices, separation of duties, and a broad range of other techniques. Administrative safeguards are essential to complement physical and technical safeguards to ensure that the risks to automated information systems are reduced to an acceptable level.

Agencies have weaknesses in key administrative safeguards. One of the major threats to any automated information system is from inside the organization, namely, intentional and unintentional actions of employees. For instance, separation of duties is

BEST COPY AVAILABLE

intended to prevent unauthorized actions by employees. We found that written procedures and/or organizational structures did not always provide for separation of duties necessary for the execution of critical functions.

We also found five instances where data processing security procedures were not tested to ensure that they were effective. Also, agencies responded that passwords were required for 24 systems. However, we found three cases where passwords were not required to be changed.

Chart 4 shows the potential effect of not having selected safeguards in place. For example, without audit trails there are limited means to track actions or security violations or to determine quickly, the impact of unauthorized access to the system or agency. Without testing security safeguards there is less assurance that they are working.

In conclusion, no agency met all management responsibilities, and only five systems evaluated contained each of the safeguards studied. Improvements are needed in both of these important areas. With regard to making these improvements, officials of several agencies cited reasons for the shortfalls in implementing management responsibilities and security safeguards. These included a lack of (1) management commitment, (2) funds and resources, and (3) assistance in implementing policy and guidance. Therefore, Mr. Chairman, these determinations lead us to conclude that the automated information systems studied are vulnerable to threats and their potential effects. It is the responsibility of agency heads to ensure that policy and guidance emanating from the responsible central agencies are implemented. Our survey indicates that such policy and guidance often are not implemented.

- - - - -

This completes my prepared remarks. We would be pleased to answer any questions that you may have.

BEST COPY AVAILABLE

OBJECTIVES, SCOPE AND METHODOLOGY

On August 7, 1984, the Chairman, Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology requested that we assess the extent to which selected federal agencies are protecting the data in automated information systems for which they are responsible. For our review, we selected 25 mission-critical automated information systems at 17 federal civil agencies. After selecting the agencies and the systems, we met with Subcommittee staff to obtain their concurrence.

To assess the security status of these systems, we used existing criteria and two questionnaires which focused on two interrelated issues to collect relevant information about the security status of the systems.

One issue primarily involved Office of Management and Budget (OMB) policy reflected in OMB Circular A-71, Transmittal Memorandum No. 1, which focuses on automated information systems security management responsibilities. Criteria used to develop this management questionnaire were supplemented by National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS), Office of Personnel Management (OPM) instructions, and expert opinion.

The second questionnaire focused on the actual security safeguards for mission-critical automated information systems. The questions were developed primarily using the Department of Defense (DOD) Trusted Computer System Evaluation Criteria, NBS Federal Information Processing Standards, and expert opinion including NBS, National Computer Security Center (NCSC), and the Department of Defense Computer Institute (DODCI).

We also developed scenarios of the potential effects of problems in areas such as those covered in the aforementioned questionnaires. These scenarios show how systems are vulnerable when certain management responsibilities and security safeguards are not in place. We validated these potential effects with the NBS, the NCSC, and the DODCI.

Follow up interviews were held at several agencies to validate the responses received from the two questionnaires, and exit conferences to present the results of our survey were held with all agencies. This survey did not involve testing the effectiveness of the management responsibilities and safeguards.

The following appendices reflect the aggregated detailed results of the survey and disclose (1) a list of the 17 agencies surveyed, (2) aggregated survey results of the questionnaires including general information; management responsibility elements; physical, administrative, and technical safeguards; and other

BEST COPY AVAILABLE

security information obtained from the questionnaires, (3) management responsibilities and scenarios of potential effects of weaknesses in the responsibilities assigned, and (4) physical, administrative, and technical safeguards and scenarios of potential effects of safeguards not in place. Appendix III identifies the potential effects of weaknesses in management responsibilities, such as those identified in appendix II, and appendix IV identifies the potential effects of weaknesses in security safeguards also shown in appendix II.

BEST COPY AVAILABLE

 APPENDIX I

FEDERAL AGENCIES INCLUDED IN AUTOMATED INFORMATION SYSTEMS SECURITY SURVEY

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF COMMERCE

DEPARTMENT OF EDUCATION

DEPARTMENT OF ENERGY

DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF INTERIOR

DEPARTMENT OF JUSTICE

DEPARTMENT OF LABOR

DEPARTMENT OF STATE

DEPARTMENT OF TRANSPORTATION

DEPARTMENT OF TREASURY

FEDERAL RESERVE SYSTEM

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

SMALL BUSINESS ADMINISTRATION

VETERANS ADMINISTRATION

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS [1]
GENERAL INFORMATION	
Length of Time this Information System has been Operational	
Less than 1 year	1
At least 1 year	2
At least 5 years	11
10 years or more	11
People/Institutions having System Accounts	
0	2
1 - 25	5
26 - 200	5
201 - 1,000	6
1,001 or more	7
MANAGEMENT RESPONSIBILITIES	
Risk Management	
Risk analysis within past 5 years	19
Risk management procedures	14
Risk analysis used to determine current level of security control	14
Contingency Plans	
Plan exists	18
Plan is tested	9
Assigned Responsibility for Computer Security	
Security officers' position description contain security responsibilities	20
ADP personnel position descriptions contain security responsibilities	4
Information Systems Security Officer (ISSO) Assigned	23
Written Procedures for Computer Security	
Facility procedures	22
Overall policies & procedures	13
ADP Personnel Security	
Position sensitivity levels designated	17
Use of new OPM regulations	2
Use of old OPM regulations	18

[1]Systems do not always add to 25 because of non-response to certain questions.

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Computer Security Costs	
Budgeted and accounted for separately	1
Computer Security Training Program	
Policies and/or procedures	19
Formal program	2
Audits and/or Evaluations	
Evaluation performed	22
Independent and within past 3 years	19
PHYSICAL SAFEGUARDS	
Physical Perimeter	16
Physical Access	All
Electronic Monitoring	
Computer room	7
Computer room access halls	9
Building access	13
Badge Entry	23
Security Guards	22
Cypher Locks	14
Various Detectors	
Metal	3
Smoke	23
Heat	24
ADMINISTRATIVE SAFEGUARDS	
Written procedures for safeguarding this system's information contained on microcomputers and related storage media at the information center	2 *
Written procedures for safeguarding this system's information while it is being transmitted between the microcomputers and related storage media at the information center	1 *

*Not applicable to all systems reviewed.

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
ADP positions at the information center designated in terms of sensitivity	17
Federal Personnel Manual, Chapter 732, used for ADP positions at the information center	3
Background investigations in compliance with Federal Personnel Manual 732 for information center personnel	
Data entry personnel	15
End Users	12
Security officers	21
Systems Programmers	20
Contractors	16
Systems Analysts	17
Application Programmers	18
Computer Operators	18
ADP Auditors	11
Data base Administrators or Managers	18
Communications personnel	16
For the ADP personnel at the information center, to what extent does the organization comply with the background investigations provisions of OPM's FPM, Chapter 736	
To little or no extent	1
To some extent	None
To a moderate extent	2
To a substantial extent	10
Fully	9
Tested the Physical, Administrative and Technical Procedures	20
Review Audit Trail Information	10
Formal Security Procedures Manual at the Information Center	
For all systems	16
For this system	3
Separation of Duties in the Following Areas	
Input processing	21
Error correction	21

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Software design, development, test and operation	19
System programming and data base administration	21
Computer operations, telecommunications, and maintenance	24
Computer and telecommunications security	19
System access - retrieval	18
System access - update processing	19
Unescorted System Maintenance Personnel Access to System	13
Unescorted System Maintenance Personnel with Clearances at Highest Level of Data Processed	10
Inactive Accounts Purged?	
Never done	2
Upon reassignment or employment termination	21
Upon termination of a system account	9
At least once a year	14
Longer than a year	1
Frequency of Password Changed for this System	
Not required to be changed	3
At least every 3 months	9
Between 3 and 6 months	6
Between 6 and 12 months	5
More than 12 months	1
Passwords are Changed by	
User	12
System administrator/security administrator	11
System, centrally managed by an administrator	4
System, independent of an administrator	1
Passwords are Distributed by	
Letter	8
Electronically from the system	3
Discussion with ISSO	7
User creates and maintains	11

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
TECHNICAL SAFEGUARDS	
Identification and Authentication	23
Audit Trails or Logs	10
Discretionary Access Controls (Authorization)	24
Restrictive Markings Limit Access to Data	10
Users have Access to all Data in the System	2
Software Changes are Recorded	
Manually	20
Automatically	15
Not recorded	None
No changes are allowed	1
Uses Add-On Security Software	17
Users are Automatically Informed at each Log-on of the Time and Date of Last Log-on	5
Users are Automatically Notified at each Log-on of Invalid Attempts to Use the System Account	2
Use Encryption (encoding) Techniques	Few*
TELECOMMUNICATIONS SECURITY	
Off-hours Access Via Leased or Dial-up Lines	16*
Anti-Hacker Devices	
Dial back capability	Few*

*Not applicable to all systems reviewed.

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Never Permit Maintenance Personnel to Perform Hardware/Software Diagnostics Via Unclassified Dial-up Lines	13*
Lines Leaving Afforded Transmission Protection	Few*
CONTRACTOR SECURITY	
Role of Contractors for the Hardware Operation and Maintenance	
Operated and routinely maintained by agency personnel	2
Operated by agency personnel but routinely maintained by contractor	14
Operated and routinely maintained by contractor	9
Operated by contractor but routinely maintained by agency personnel	None
Role of Contractors for the Software Operations and Maintenance	
Operated and routinely maintained by agency personnel	14
Operated by agency personnel but routinely maintained by contractor	3
Operated and routinely maintained by contractor	7
Operated by contractor but routinely maintained by agency personnel	None
CONTINGENCY PLANS	
Center Experienced an Unplanned Operational Discontinuity	19
Unplanned Discontinuity Occurred	
Less than 1 year ago	13
From 1 to 3 years	6
More than 3 years ago	None

*Not applicable to all systems reviewed.

BEST COPY AVAILABLE

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Uninterruptible Power Supply	13
Type of Uninterruptible Power Supply	
Battery	1
Generator	2
Both generator and battery	12
SECURITY MANAGEMENT APPROACH	
Staff Effort Devoted to System Security Functions	
None	None
1/2 staff year or less	7
More than 1/2, but less than 1 staff year	4
1 staff year, but less than 3 staff years	5
3 staff years, but less than 5 staff years	3
5 staff years or more	5

BEST COPY AVAILABLE

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
Agencies should establish an agency computer (automated information) security program at a management level commensurate with responsibilities involved and with sufficient authority to enforce established requirements.	AGENCY SECURITY PROGRAM	
	An agency computer and telecommunications (automated information) security program at appropriate management level.	Inadequate program can lead to inadequate implementation and control.
	Authority to enforce program requirements	Insufficient authority tends to perpetuate known weaknesses and prevent identification of unknown weaknesses.
The program should		
1. Establish a formal ADP System Security Organizational Framework that	1 ORGANIZATIONAL FRAMEWORK	
	Formal (written) responsibility and authorities that	
—assign responsibilities and authorities for security of data processing installations, security officers, users, operators, and contractors via procedures and contract clauses.	are clear and not overlapping or fragmented.	Unclear, overlapping and fragmented responsibilities can lead to organizational procrastination in identifying and implementing safeguards and duplication of effort. Control problems go undetected or uncorrected for periods longer than necessary.
	clearly define responsibilities of (see next page)	

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	—data processing installation personnel,	Effective management can be negated if security is not perceived as part of total job responsibility and stated in employee position descriptions. Causes procrastination and duplication since the position description is a major source of accountability and enforcement.
	—managers,	(SAME EFFECT AS ABOVE)
	—primary users,	If responsibilities and accountabilities are not spelled out in position descriptions, persons/organizations most knowledgeable of data sensitivity and possible harm or loss may not be involved in automated information systems security decisions.
	—monitoring entities (evaluation),	Adequacy of automated information systems security program and controls may not be evaluated, if position descriptions are devoid of responsibilities for automated information systems security.
	—contractors,	Insufficient contract clauses specifying contractor responsibilities and authorities causes enforcement, procrastination, duplication and other problems.
	—security officers.	Position descriptions that do not clearly describe responsibilities and authorities for automated information systems security can cause unresolved clashes with ADP operations and users. Clashes among security officers also may not be resolved. Needed controls can go unimplemented or problems undetected.

BEST COPY AVAILABLE

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
2 Formulate a comprehensive ADP Systems automated information systems security policy.	2 ADP SYSTEM SECURITY POLICY The existence of policy.	Absence of, or unclear policy can result in no clear organizational position. Controls could not be implemented or enforced because of confusion.
1 Develop written comprehensive ADP systems security standards and procedures applicable to all organizational units responsible for processing and protecting data.	3 STANDARDS AND PROCEDURES For developing, implementing and operating the automated information systems security program. They should cover	
	—appropriate organizational entities and people.	If entities and employees are uninformed of their role for effective security, control violations or problems can be created.
	—risk management and data sensitivity.	Failure to require and use data sensitivity and risk management can lead to overprotection or underprotection. Appropriate levels of controls to afford cost-effective protections can not be determined.

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	—budgeting and costing.	Lack of security budgeting and costing can result in uncontrolled overprotection, failure to identify inadequate controls, resource conflicts leading to inadequate safeguards, inability to monitor cost-effectiveness of controls, compare costs, monitor plans, etc.
	—training.	See "training and awareness programs."
	—security planning.	Inadequate planning can lead to inadequate program implementation and exposed vulnerabilities because of inadequate controls.
	—types of data and processing covered.	Sensitive data in hands of those unaware of protection requirements is a vulnerability. Importance increased because of end user computing. Information processes not covered also represents a vulnerability.
	—mechanisms for corrective actions (reporting and follow up).	Poor or no procedures or mechanisms for assuring effective corrective actions can lead to control problems detected which are not always corrected, or corrective actions which do not work effectively.

BEST COPY AVAILABLE

APPENDIX III

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
4 Require the formulation and testing of backup and recovery contingency plans.	4 CONTINGENCY PLANS	
	The existence of plan.	Mission can be impaired with significant discontinuity if no plan exists. Human safety can be endangered in some applications.
	Testing of plans.	If existing plans are not tested, backup plans may not be effective, again leading to potential mission impairment.
5 Assign responsibilities for conducting periodic risk analysis and implement cost effective technical, administrative, and physical safeguards based on a risk management approach.	5 RISK MANAGEMENT	
	Responsibilities assigned for conducting periodic risk analysis.	Unclear assignment of responsibilities may result in not conducting or improperly conducted risk analysis. This can impact control effectiveness since it forms basis for selecting proper mix of controls.
	Use of risk management approach for implementing controls.	Insufficient compliance in performing risk analysis and using risk management approach can lead to not identifying or implementing cost effective controls (underprotection). Costly overprotection (without closing vulnerability) is also a possible result.
	Determining data sensitivity and data sensitivity levels.	If data sensitivity determinations are not being made or levels not established, then risk management can result in inadequate controls for highly sensitive data leading to high risk (underprotection). Data sensitivity, including criticality and value, is a key factor in risk management. Its absence negates the risk management process.

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	Elements of risk management approach employed (data sensitivity, vulnerabilities, threats, risks, alternative safeguards, costs, relative effectiveness, etc.).	Not using risk management approach can result in cost effective safeguards not identified or implemented. Over or underprotection is possible while vulnerabilities remain.
	Frequency of risk analysis and changes in circumstances.	Major changes in circumstances may create new vulnerabilities, threats and increased risks which need to be identified and safeguarded. If risk analysis is not done periodically or when circumstances change (modification, new site, employee changes, and changes in processing procedures) they may not be identified.
6 Establish personnel security policies for screening all individuals participating in design, operation, maintenance, or having access to data in federal computer systems.	6 PERSONNEL SECURITY Existence of policies for screening personnel.	Absence of policy may result in overscreening or underscreening.
	Responsibilities for implementing policy.	Unclear responsibilities can result in organizational procrastination or duplication. Personnel control (screening) may be inadequate.
	Effectiveness of implementing policy.	Ineffective policy may result in overscreening or underscreening.

APPENDIX III

BEST COPY AVAILABLE

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	Designation of sensitive positions	If ADP positions are not designated in terms of sensitivity, then there may be an inappropriate basis for performing background checks. A major threat to systems is employees. Employees in sensitive positions can exploit controls and commit fraud and abuse.
	Use of sensitivity levels for ADP positions.	Levels of sensitivity needed are for managing extent of personnel control.
	Background investigations performed	
	for all applicable personnel.	Employees are a major threat to systems. If checks are not performed for all applicable personnel there is insufficient basis for trust. Controls can be exploited.
	updates of background investigations.	Since people and circumstances change, infrequent updates of investigations may result in not identifying a new threat.
	clearance information used in risk management.	Threat of unauthorized access is increased if clearance information is not used in performing risk management.

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
7 Establish management control process	7 MANAGEMENT CONTROL	
a) to budget and account for computer and telecommunications security costs and resources, for planning, risk management, and control purposes.	Budgeting and accounting and/or estimating where appropriate for security costs and resources.	Lack of awareness of security costs and related cost components for systems and agencies can result in uncontrolled overprotection, failure to identify inadequate controls, and inability to monitor cost-effectiveness of controls, etc.
	Use of budget and cost for planning, and control.	Management planning and control is not fully effective without knowledge of costs.
	Use of budget and cost in risk management.	Risk management is not effective without knowledge of costs of alternative controls.
b) to evaluate risk analysis.	Agency evaluation of risk management approaches.	Risk management approaches used may not be appropriate if not evaluated. Impact on control effectiveness is a possible result.
	Agency evaluation of risk analysis conducted.	Risk management effort may not be adequate if not evaluated. Impact on control effectiveness is a possible result.

APPENDIX III

BEST COPY AVAILABLE

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
c) involving procedures and mechanisms to assure that exposed vulnerabilities or corrective actions recommended are adequately and effectively acted on.	Follow up on recommendations.	Failure to act on recommendations to correct problems (vulnerabilities, etc.) because of poor or no procedures or mechanisms for taking corrective actions, can result in vulnerabilities which remain (unsecured), and controls in place which may not be totally effective.
8 Establish an annual security plan.	8 ANNUAL SECURITY PLAN	
	Existence of plan	Inadequate planning can lead to inadequate control.
9 Establish comprehensive automated information Security Training and Awareness Programs and manage it to assure its effectiveness.	9 TRAINING AND AWARENESS PROGRAMS	
	Existence of training program, which should include	Employees responsible for sensitive data, if untrained, may be unaware of controls available, responsibilities, potential impacts, etc. Existing controls may not be effective.
	audience.	If user awareness of vulnerabilities and controls are not a primary target, then the user may be unaware of how to effectively implement controls.
	training content (topics).	Proper subjects not presented to employees can render controls ineffective.

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL IMPACT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	feedback to determine effectiveness (testing etc.).	Making an assumption that training is effective without requiring and receiving feedback can result in inadequate controls implemented by employees or commission of errors causing damage.
	training of security officer.	Inadequate training of security officers can lead to inadequate controls.
10 Establish agency program for conducting audits and evaluations to determine the compliance with and cost effectiveness of the security program.	10 AUDITS AND EVALUATIONS (MONITORING)	
	Existence of periodic independent audits.	Without independent evaluation, there is no validation that cost effective controls exist.
	Certifications and recertifications.	Without certification and/or recertification, inadequate controls may continue to exist.
	Implementation of recommendations.	Without sufficient follow-up, needed controls and safeguards may not be implemented or may not work effectively.

APPENDIX III

BEST COPY AVAILABLE

BEST COPY AVAILABLE

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL IMPACT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
11 Actively monitor the application of computer and telecommunications security by contractors performing data processing for the federal government.	11 SECURITY BY CONTRACTORS	
	Monitoring of contractor security measures.	Without monitoring, needed controls may not be implemented. Also controls implemented by contractor may not be effective.
	Procedures for protecting assets when contractors change.	Vulnerability is created by changes in contractor/ employees. Assets and data are vulnerable.

44

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Physical		
Physical Controls	Physical security controls should exist and be adequate.	Poor physical security allows unauthorized access to information resources. Physical security is becoming increasingly important because of portability and size of micro-computer systems.
Administrative		
Testing Procedures	Security procedures and features should be tested.	Without independent testing of security safeguards there is less assurance that controls are in place and/or working effectively.
Separation of Duties	Procedures and/or partitions should exist to ensure separation of duties.	Major threat is from inside the organization. Separation of duties is a key internal control (administrative safeguard) to prevent internal intrusion without collusion.
Position Sensitivity Levels	Personnel positions at the information (computer) center should be designated in terms of sensitivity.	If positions are not designated in terms of sensitivity there is little basis for decisions about the level of access to be granted to individual employees, the extent and nature of background checks, duties to be separated, procedures for disgruntled employees etc.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Position Sensitivity Designation	OPM FPM Chapter 732 INSTR 311 should be used to identify sensitivity levels for ADP and other key positions.	Without using a standard to identify sensitivity levels for federal personnel involved in ADP processing, differences in criteria can lead to unidentified potential threats.
Background Investigations	Background investigations should be performed in accordance with OPM FPM 732, Chapter 736.	Insufficient background investigations may result in the failure to disclose a primary threat to the information system.
Update Background Investigations	Updates of background investigations should be performed periodically.	Circumstances and habits change and updates are needed to disclose significant changes which may pose a threat to the system.
Change Passwords	Password changes should be required and performed frequently.	Not changing passwords leave systems vulnerable to attack by former employees.
Generation of Passwords	Users should not generate their own passwords when they are changed (unless NBS FIPS is used).	Undertrained users may not be sufficiently aware of the pitfalls of using passwords that are easy to break. Users may be inclined to use birth date, wedding anniversary, names, short passwords or other personal identifiers that are more easily broken based on personal knowledge of the individual. Use of NBS FIPS is needed for sensitive systems.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Audit Trails Reviewed	Reviews of audit trails for security should be made, performed frequently and effectively.	Existence of an audit trail (a technical control) is not sufficient. Frequent reviews are needed to determine if irregularity exists. Audit trails are not an effective violation detection mechanism unless such reviews are effectively performed and detection is followed up.
Microcomputer Procedures	Procedures should exist for protecting data while residing on microcomputers and for protecting information being transmitted between microcomputers and mainframe computers.	Without procedures, data from or for system may not be protected on microcomputers. Sensitive or costly information on microcomputers must be protected regardless of its source. Sensitive information being transmitted between computers must be safeguarded to an extent dependent on risk management.
Security Procedures Manual	There should be a formal security procedures manual at the information center (computer center).	Without formal procedures, training and actual use, implementation of control can be haphazard. Some employees, e.g. new hires, may be unfamiliar with controls and accidently violate them.
Restrictive Markings	There should be restrictive markings that limit access to data at the information center (computer center).	Without restrictive markings for sensitive data, employees may not be aware of its sensitivity, and may not implement effective control in its handling and use.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Clearances-maintenance personnel	Unescorted maintenance personnel who have access to the system should have appropriate clearances or authorizations.	Maintenance personnel represent a threat of unauthorized access to the system. Escorts and clearances are basic safeguards against this threat.
System Accounts Purged	The status of individual system accounts should be reviewed periodically and inactive accounts purged.	Access accounts should be up to date to be an effective technical control. Reviews should be done frequently and when an individual is reassigned or terminated. Failure to review and purge inactive accounts can lead to use of accounts of terminated or reassigned employees to access the authorization.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Technical		
Discretionary Access Control	Software or hardware protection should exist to protect user files via access control lists, file passwords or class of user. (LEVEL C1)	May not have the required technical access control needed to deter unauthorized access (e.g. extent of complexity, sophistication and cost), which should be dependent on risk levels, and risk management. The overall system effectiveness of technical access controls rest to a large degree on the balance of administration of password updates and changes, personnel and other administrative controls with the supporting technical controls. Poor administration of these technical controls can potentially result in their circumvention leading to system violation.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Identification and Authentication	The system should possess identification/ authentication features e.g. log on/password which uniquely identifies an individual and is protected by the software/hardware from unauthorized acquisition and modification. (LEVEL C1)	The system does not identify the source of authorization and identification e.g. institution or user. This is needed to determine potential sources of intrusion, leak, usage history and to effectively validate user's authority. Passwords and other identification and authentication mechanisms are not protected and are more easily disclosed.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF TECHNICAL CONTROLS	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Audit	System should have capability to record in an audit trail or console log attempts at log on, file accesses, network access, security violations, user privilege changes, security review actions, and console operator actions. It should record users actions by individual identity and/or security level. (LEVEL C2)	No means to track system/ network accesses or security violation. Unable to monitor actions being taken by persons responsible for performing security reviews. Unable to identify user privilege changes by computer. Audit trail weaknesses limit the means for detecting unauthorized access to system and to determine, quickly, the impact on the system and agency. Can also impede effective recovery. Poor administrative control related to audit trail (e.g. failing to review audit trail frequently, or at all for security purposes) could render this detection, and correction technical control ineffective.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Uninterruptable Power Supply	Uninterruptable Power Supply should be used where justified.	Mission can be degraded or impeded and data can be lost.
Transmission Protection	Telecommunications lines should be encrypted or physically secured where justified.	Transmission over telecommunications lines represents a vulnerability to the unauthorized access, monitoring, or altering of automated data.
Log-on Notification	The system should inform user at log on of prior (last) log on date and time.	Without control for sensitive systems, user is not aware of unauthorized use of his/her access code. Control could lead to the identification (detection) of unauthorized access to system.
Invalid Attempts Notification	The system should notify the user (at log on) of invalid attempts to use system accounts.	Absence of control could delay or prevent timely detection of unauthorized access and delay or prevent timely apprehension of perpetrator. Notifying security officers may be even more desirable.

BEST COPY AVAILABLE

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Encryption	Encryption should be used to secure sensitive or compartmented data.	In critical or particularly sensitive systems, encryption is dependent on risk management. However encryption of key data such as passwords, as well as sensitive data (at certain levels) may be a cost effective control.
Error Reports	The system should produce reports that specify actual or estimated error rates.	Integrity and accuracy are significant considerations in system security. Errors and sources need to be detected and corrective action taken. A system can detect and/or correct many types of (but not all) errors. Erroneous data can lead to mission impairment, uneconomical actions, and human safety problems.

BEST COPY AVAILABLE

COMPUTER SECURITY MANAGEMENT EVALUATION

Management Responsibilities*	Number of Systems Meeting Requirements
Risk Management	8
Training	2
ADP Personnel Security	2
Assigned Responsibility	4
Budgeting and Accounting for Security Cost	1
Contingency Plans (exist and tested)	9
Independent Evaluation or Audit	19
Written Procedures	11

*Elements of criteria used to evaluate agency implementation of each of these management responsibilities are shown in appendix II.

CHART 1

BEST COPY AVAILABLE

 APPENDIX V

POTENTIAL EFFECTS
MANAGEMENT RESPONSIBILITIES
NOT IN PLACE

RESPONSIBILITY	POTENTIAL EFFECT
Lack of Risk Management	Controls missing and/or not cost effective.
Lack of Continuity of Operations Plan and Testing the Plan	Mission can be impaired and human safety endangered.
Lack of a security training program	Employees unaware of controls needed.
Lack of independent audits and evaluations	No validation that controls exist.

CHART 2

BEST COPY AVAILABLE

APPENDIX V

PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY SAFEGUARDS

	SYSTEMS HAVING SAFEGUARDS
PHYSICAL SAFEGUARDS	
Physical Perimeter	16
Entry by Badge or Cypher Lock	24
Use of Security Guards	22
Use of Smoke and/or Heat Detectors	24
TECHNICAL SAFEGUARDS	
Identification and Authentication	23
Audit Trails or Logs	10
Discretionary Access Controls (Authorization)	24
ADMINISTRATIVE SAFEGUARDS	
Separation of Duties	15
Physical, Administrative and Technical Procedures Tested	20
Audit Trail Information Reviewed	10
Passwords Required to be Changed	21
HAVE ALL SAFEGUARDS	5*

*Although these systems contained all evaluated safeguards, they may still be vulnerable because (1) GAO evaluated selected safeguards only, and (2) all evaluated management responsibilities were not implemented. GAO does not know how vulnerable the systems may be because this survey did not involve testing the effectiveness of the safeguards.

CHART 3

BEST COPY AVAILABLE

APPENDIX V

POTENTIAL EFFECTS
PHYSICAL, ADMINISTRATIVE, AND TECHNICAL SAFEGUARDS
NOT IN PLACE

SAFEGUARD	POTENTIAL IMPACT
Lack of Physical Safeguards	Unauthorized access possible.
Lack of Testing Security Procedures	Less assurance that safeguards are working.
Lack of Separation of Duties	Threat of employee fraud and abuse is increased.
Lack of Audit Trails	Detection of unauthorized access limited.

CHART 4

BEST COPY AVAILABLE

Mr. GLICKMAN. Our next witness is Mr. Richard Kusserow, inspector general of the Department of Health and Human Services.

I would state again for the record how important it is for Congress to have an agency like the GAO, which is independent but basically subject to our control, to do this kind of work. I think they have done a splendid job.

Mr. Kusserow, I know you have been before our committee before. We appreciate your coming back. You may read your statement. The entire statement will appear in the record, so you may proceed as you wish.

STATEMENT OF RICHARD P. KUSSEROW, INSPECTOR GENERAL, DEPARTMENT OF HEALTH AND HUMAN SERVICES, ACCOMPANIED BY JOHN I. MOLNAR, SENIOR ANALYST, AND VINCENT MAZZUCA, DIRECTOR, EDP AUDIT DIVISION

Mr. KUSSEROW. Thank you, Mr. Chairman. I do appreciate the opportunity to come back before your committee to talk on this very vitally important subject of computer security in the Federal Government.

I come as the inspector general for the Department of Health and Human Services, which has some 300 programs which are all dependent upon these systems. But I also come as chairman of the computer security project of the President's Council on Integrity and Efficiency, which looks at computer security across the entire Federal Government.

Accompanying me today is John I. Molnar, who is senior analyst and project leader for one of the reports that I am submitting to you today. Also along with me on my left is Vincent Mazzuca, who heads up our EDP Audit Division.

I have a full written statement for the record, as well as two reports and briefing charts, all of which I would like to submit for the record, and then summarize if I may.

Mr. GLICKMAN. All of your information will be included in the record.

Mr. KUSSEROW. Thank you, Mr. Chairman.

Today no business or entity can effectively operate without the assistance of computers, least of all the Federal Government, which has more than 20,000 main frame computerized system operating at the present time, with additional ones being added every day. We have become almost dependent upon this technology to operate the Federal Government. Without the computer, the Government could not fulfill many of its missions such as operating the Social Security Administration, Medicare, various health research projects in our department, and so forth. By 1990 we will probably also have in place another half million micro and minicomputers which are freestanding, making our dependence on technology even greater than what it is today.

Computer security is primarily an agency responsibility and is a major concern of the IG community, of which I am a member. Agency managers must implement computer security policies and practices, and internal auditors and investigators must audit the controls or investigate abuses of the system. To do this, however, we need a thorough knowledge of the vulnerabilities of the comput-

BEST COPY AVAILABLE

erized systems that are operating in the Federal Government. Then also we realize that, in order to gain more information about the computer systems themselves, as well as their vulnerabilities, we would have to take a Government-wide look at what exactly was operating in the Government.

Since 1983, the President's Council on Integrity and Efficiency through the computer security project has engaged in two major comprehensive studies relating to the vulnerability and integrity of our computerized systems.

I would like to summarize those studies. In our 1983 study, which was unique in the fact it was probably the most comprehensive study of any system not only in the Government but even in the private sector, we used the survey instrument development by the American Institute of Certified Public Accountants for their review of the banking and insurance industries. They had a year's head start on us, and we finished a year ahead of them. So, it shows once again that, when the Government wants to put their shoulder to the wheel, we can out do the private sector.

We did look at all cases of computer fraud and abuse that had been identified in the Federal Government between 1978 and 1982. Then we analyzed these cases, which gave us a better idea of some of the vulnerabilities that existed. For example, we found that fraud cases primarily involve theft of cash or diversion of assets, usually through input manipulation in the benefit or payroll systems. Most abuse cases involve the use of computer time for outside business or entertainment.

Most perpetrators were nonsupervisory, data entry employees earning $20,000 a year or less. Therefore, the 90 percent of the problems that we encountered in the Federal Government of fraud and abuse involving our computers were in the areas that are most easily correctable. So, indeed, we have as bad news a lot of problems in our computerized system. The good news is that they are correctable. And they are correctably fairly easily if in fact we would just make a more heavy commitment in this area. Data input problems can be significantly reduced with very limited proper controls being placed in the systems.

We did confirm that losses ranged up to about $117,000 per case, although the actual losses were thought to be higher. This again is in the 1983 study.

Most of the cases were detected by accident and by fellow employees. This is very significant in this respect, Mr. Chairman. It meant that these individuals were not caught by controls working to show an aberration in a system and allow people to go after it. Also the people who encountered it were not the managers of the computerized systems. They were not the computer security officers. They were not the auditors themselves in the agencies. They were fellow employees. This should tell us that, when the majority of the problems are being encountered by accident and by fellow employees, that leaves something to be desired in both controls and in the people who have a responsibility for overseeing the systems.

Finally, in our 1983 study we found that our respondents, who were people actually dealing with the problem in an oversight capacity within the agencies, were not very knowledgeable about controls, systems reviews, or audits. This is evidenced by the fact that

BEST COPY AVAILABLE

most could not even respond to our questions with regard to what kind of vulnerability assessment or risk analyses had been done, what kind of controls were in place, or when was the last time the systems had been reviewed. Most of them could not even answer those questions in a logical fashion.

Therefore, at the completion of that phase of our review of the Federal Government's vulnerability to having their systems violated, we really felt that we had created more questions than we actually answered. We thought it would be important to go back to the perpetrators themselves to see if we could learn how and why they committed their crimes, and also to identify through them some of the systems vulnerabilities that were not really apparent in the first phase of our study.

So, our second review really focused on the perpetrators themselves. We interviewed 46 perpetrators, who were caught and convicted for engaging in computer crimes. We used both the original study and supplemented it with additional perpetrators that had been caught subsequently.

We found in almost every instance that the perpetrators had been employees of the Federal agencies, or were in State-administered, or locally administered Federal programs or were in private agencies administering Federal programs. We did not find any hackers among our list because we focused on those people that defrauded the systems, and we have come to realize that hackers represent primarily a privacy concern. We are focusing on separate concerns with regard to the hacker problem.

In addition, we found that the perpetrators had been identified within their agencies as good, young employees. Their average age was 30 years at the time that they committed their crime. If you measure that against the average age of the Federal employee, which is 40, you can see that they are younger than the average. Also, they had been with the agencies for approximately 5 years on average.

During their employment, three-fourths of the perpetrators had been recognized as good performers by being promoted at least once. Two-thirds had reported having average performance appraisals, with one-fourth receiving performance awards for being above average. In fact, four of the perpetrators had gotten awards for designing and implementing the systems that they ultimately stole from.

We were surprised to discover that one-fifth actually had criminal records at the time they were hired by the agencies. This is both the Federal and State and local agencies. Some were even hired under programs for ex-offenders. I will admit candidly that one of them, in our Department, was hired under the convicted offender program and then put in payroll. Then we were surprised to find that he stole $40,000.

Most noted their criminal records on their job applications, but a few concealed their criminal records from the agencies that hired them. We think this is an area of vulnerability that we should really look at. We are certainly all in favor of giving convicted offenders a new opportunity, but it seems to me that we might have some sense as to how we want to place them once we hire them. Maybe we wouldn't want to put them right in the center of payroll.

BEST COPY AVAILABLE

These perpetrators' jobs gave them the access they needed to commit the crimes. Almost three-fourths worked in benefit programs and were in position to cause funds to be issued in a way that would advantage themselves. The jobs varied greatly, from secretaries and clerks to programmers. They also included some senior managers, and in one case we actually had a criminal investigator who found a way to manipulate the system.

Most positions occupied by the perpetrators can be grouped into three common types. First, we have about one-third who were case workers. These are individuals who worked in benefit programs and who made decisions on eligibility and payments and could influence the system in such a way to advantage themselves financially.

One-fourth were computer personnel. Most of these were data entry technicians, but a few were programmers and systems analysts. As I point out, we even had some that were in payroll or financial payment systems.

Another quarter were strictly clerical positions, that were primarily responsible for managing paper, they did have access to the computer systems as part of their job.

One-quarter of all the perpetrators were supervisory positions. This is consistent with our original study.

Importantly, 40 percent did not have direct hands-on access to the computer. Most of these people were individuals who completed forms which were forwarded to data entry technicians who in turn entered it into the system.

The perpetrators used three predominant schemes to commit their crimes. The most common was to modify existing case files in an ongoing payment system such as Social Security, unemployment insurance, or even payroll. A typical modification was to change the address to which the check was sent after the payee died or became ineligible. So, they were able to convert the check to their own personal use.

The second most common scheme identified in our study was to load false claims or bills into a financial system such as an administrative voucher system or a system for reimbursing doctors, beneficiaries, or contractors.

Another common scheme was to create false cases in a benefit or payroll system. This was the most difficult scheme to develop because it required the perpetrator to create a false identity for the bogus case. It was more difficult to do in most systems.

A somewhat surprising finding was that a majority of the perpetrators used co-conspirators. In our first study, we found that most had acted alone. We subsequently found in talking to the perpetrators that indeed they had not acted alone, that most people involved in this kind of a crime did in fact have co-conspirators. In fact, during the course of this study, we identified 50 additional co-conspirators in the interview process we had with the perpetrators. In one case we had an individual who was serving time in a penitentiary while his coconspirators, who were never identified, were paying their guilt money for this guy's penalties that were assigned by the court.

The kinds of people who were coconspirators were sometimes people outside the organization who were used to receive cash or

55-930 0 - 86 - 3

BEST COPY AVAILABLE

cash checks themselves or use false identification. In the other major category of co-conspirators generally were fellow workers who either provided moral support or helped bypass controls where there was segregation of duties.

Other data that came from these cases also provides some perspective on computer crime. The average loss we established to be about $45,000, but ranged up to $360,000, which was considerably more than what was shown in the overt investigative records of those individuals.

The period of criminal activity lasted about 6 months, that is, the criminal activity and transactions went on about 6 months before they were caught. We actually had one case that was identified that went on for 6 years.

On average, the perpetrators entered eight illegal transactions into the computer, but one case involved almost 200. So, each one of these illegal transactions was a separate criminal act. Thus, you can see that we are talking about someone who doesn't do it one time, but does it over and over and over until caught.

When we asked the perpetrators why they committed the crimes, most reported that there were responding to some sort of specific problem or crisis and had rationalized that their crime was their only option to that situational stress. Many who had said they had personal problems volunteered they were also unhappy employees. Those who were not responding to a specific personal problem could not ignore the temptation of a vulnerable system. For example, some of the perpetrators actually found the vulnerabilities in the system in the normal course of their jobs. Others were intrigued by the computer and played to beat the system in their free time until they won.

One of the most disturbing findings from this study is that the work environment provided the perpetrators with the opportunity to commit their crime. We asked the perpetrators about computer security where they had committed their crime. Virtually all had been unaware of security efforts. Let me correct that. Virtually all of them had been aware of security efforts, but most said they had been weak. So, they made the judgment that, although there may have been security efforts in their agencies, they were weak and could not be counted upon to act as a deterrent for them to committing the crime.

For example, some said the systems didn't have individual access controls such as ID numbers or passwords or an audit trail to identify the workers with the transaction and the data base. But more commonly they said that the implementation of security features was weak. For some systems the ID numbers were workers' initials and passwords and were oftentimes issued by memorandum, which certainly doesn't sound like they were trying to keep it a secret.

I can attest also in my role in auditing the systems of our department, that we have in many cases gone out and looked at district offices of Social Security and found that the access numbers were scotch taped to the terminal so they wouldn't forget it. Of course, that makes it easy for somebody else to come along and use it. Oftentimes we find that some people would forget what their number is, borrow somebody else's, and use it from then on. So, you really

BEST COPY AVAILABLE

do not have a security system with ID numbers if those ID numbers are not controlled.

Edits and screens to detect atypical entries or transactions were often well known within the agencies, and by being were able to be circumvented .

The intent of separation of duties was often violated, either when staffing changes caused persons to be trained in both input and output responsibilities or where terminals were left unattended once brought online.

Again, all these things have been verified—putting on my auditor hat at HHS—from our own audit studies we've done in our own department's systems.

They also told us that line supervision was weak. It was not uncommon for a perpetrator to say: no one was watching me. They also reported that either their work wasn't reviewed because they were trusted employees or the supervisers were overloaded. Also the supervisers really didn't understand the computer system because they had done their job manually and never took time to learn how to do the job after it was automated. Basically, this was a problem of—the generation that didn't grow up on Pac Man and was afraid of looking at the CRT's versus the generation that was following it and understood that. In that gap, the generational gap, we found there was a lot of problem with supervisers who just really weren't prepared to shift their understanding to automated systems.

Based upon the data collected in this and in the 1983 report, we moved to disseminate all this to all of the inspectors general in the Federal Government as well as their agencies. We made some very specific recommendations.

Among them were that we should be debriefing these perpetrators on a routine basis, not only to identify specific systems vulnerabilities, but also to enter a general knowledge of computer related crime and to ensure that no coconspirators were left undetected. In fact, at HHS we have already established that policy in that all individuals that are found to engage in computer fraud are indeed debriefed either at the time of the investigation or subsequently after conviction, and most preferably before sentencing, to determine whether in fact we left any stone untouched.

We also found that these crimes indicate a clear need to strengthen controls in the victimized systems. Existing computer security measures need to be reviewed and monitored to assure proper implementation. Better audit trails need to be built into our systems to assure accountability. The user's access within a system must be limited to the specific job responsibility.

Although implementation of controls is a management responsibility, the inspector general's office is responsible for monitoring and testing these systems. We have an EDP audit division. Unfortunately, we are one of the few agencies that has a separate division to focus on auditing computerized systems.

We have looked at a number of different systems. We find that, by showing the flag and our interest in this area, it has resulted in quite a discernible change in the attitude of management with regard to security. It has also improved the systems themselves.

BEST COPY AVAILABLE

We think also it is a very important part of this process not to wait until systems come online and are operational to audit them. We think it should be done at the time they are designing the system to ensure the fact that controls are built into the system at the time they are being constructed and not after the system comes online, finding the defects, and trying to build in controls after the fact.

Because EDP audit of developing systems is so crucial, we have focused in our own department especially on the system modernization plan at Social Security. We have devoted the lion's share of the resources in this area, so that when we do have a new system come online, it indeed will have the kinds of things that have been deficient in the existing systems.

Given that half the perpetrators work for State and local grantees or private contractors, I think we must reevaluate our guidance to such agencies to ensure that they also will have a renewed commitment to computer security. During the coming year, we will be conducting several inspections and audits. One will review computer security of Medicare carriers and intermediaries. The other will evaluate computer systems at State and local grantees to see whether or not these recommendations are being carried out and to find whether the level of low security is improving or not.

We need to ensure that program managers and line supervisors are knowledgeable about and committed to computer security by providing them with proper training. I would also add, Mr. Chairman, that we should also say indoctrination. It's not just a question of telling them that what needs to be done, but we have to convince them that in fact it does need to be done.

Our staff has participated in a number of presentations at national meetings to increase their awareness in the area. We think that we have significantly increased our auditor and investigator training on computer security to the point where they contribute in our department to reducing those vulnerabilities.

Last, given the finding that a fifth of the perpetrators had criminal records when hired, I think we must assess the effectiveness of our personnel security programs with regard to positions that have access to automated financial or payment systems or with regard to privacy matters. We are conducting an inspection in our own department with regard to those employees that have access to that kind of information.

So, Mr. Chairman, that concludes my formal comments. I stand ready to answer any questions you or the committee might have.

Mr. GLICKMAN. Thank you very much, Mr. Kusserow, for an excellent statement.

The perpetrators that you interviewed, most of them were involved in which system? Was it Social Security systems? Which specific Government programs?

Mr. KUSSEROW. Every Government program. What we did was to build on the first study, which went across the entire Federal Government. I'm speaking with two hats. One is with regard to the entire Government, and one is from my own department. The study that we've done is across the entire Federal Government, every single agency of the Federal Government. So, we had a cross-section. When we say that we have problems with claims repre-

BEST COPY AVAILABLE

sentatives, they are not just claims representatives in the Social Security Administration, but also in the food and nutrition program. We are also dealing with programs in HUD or energy assistance or any of the benefit programs that are either the federally funded, federally administered, or federally funded State or local administered.

Mr. GLICKMAN. Because in Social Security alone, you have how many claims benefit representatives out there in the country?

Mr. KUSSEROW. We have thousands. And we are also burdened by the fact that—and I don't want to panic anyone—we were operating a computerized system that was held together with beeswax, baling wire, and band-aids. In fact, when I spoke to the other Chamber last year before one of the hearings, I was asked by a Senator something to the effect: Mr. Kusserow, what we were really concerned is, how many incidents of hackers busting into the Social Security system have you encountered? And I was able to answer: Mr. Chairman, we have had not one single instance of any hacker entering into the Social Security database because we're operating such a primitive system that we don't even have dial-in capability.

So, in one sense we're very fortunate that Social Security wasn't vulnerable to hackers. But we're also very concerned that it did not have any kind of an audit trail that would permit us to identify perpetrators by doing online reviews. And therefore it's extremely vulnerable. It's critical, as we modernize the systems of Social Security, that we don't replace it with a new system that would be equally vulnerable. We must have a system that has audit trails and controls that were totally lacking in our current system.

Mr. GLICKMAN. You heard the GAO's overall assessment of computer security. I think you were in the room when they testified. You may have seen their report if you have——

Mr. KUSSEROW. I hadn't seen the report but I heard them testify, Mr. Chairman.

Mr. GLICKMAN. OK. If you haven't, we ought to get you a copy of that report.

I wonder if you would comment on their general——

Mr. KUSSEROW. I think that overall I would agree with it. The only thing I would say is I think they're unusually charitable with regard to what they found. I think it's far worse than what they intimate. The reason I say that is that I don't know what their sample was. I don't know what agencies they looked at.

We looked at it across the entire Federal Government. We found that it really ranges in terms of vulnerability, from a low vulnerability to extremely high vulnerability. The difficulty that we have in Government to this vulnerability is the fact that we operate under some assumptions that are not borne out in actuality. Certain assumptions that we had in Government were that we only need to worry about certain computers being vulnerable. Those are the systems that relate to the national security or are those that relate to payment systems, and so forth. In other areas it's not really necessary to worry about it.

What we have come to learn in recent years is that this assumption is really faulty, that indeed, anytime you keep data, we have to be worrying about its vulnerability. So, in areas like hospital

BEST COPY AVAILABLE

data, they didn't worry if they had a user friendly system. They didn't worry about anybody accessing it because they felt nobody would really want to know about a patient's record. Now we find that hackers do in fact enjoy entering systems and playing around with them. Therefore, we find that there is a vulnerability to patient records.

Similarly, in Government, even the Defense Department, which has extremely secure systems, we have found that in those area which are just engaging in day-to-day routine transactions that they felt that had low security value, they really didn't pay as much attention in that area. Yet, these are the areas that the hackers are beginning to get into it.

So, we can say that, depending upon the agencies, we either have virtually no awareness or appreciation for security, or, at the other extreme, we have a very high awareness, very good security and a very low vulnerability.

So, I would agree with GAO. My concerns are that the problem is really at a level much higher than they looked at. They said they looked at the top people in the system shop. I say that the commitment must start from the Secretaries and agency heads all the way down. That the level we have to start on. We have to go to the Assistant Secretaries or agency heads themselves, that are way above the systems area, and put the burden of accountability on them, because without having that from the top down, I don't think that we're going to lick this problem.

Mr. GLICKMAN. Your particular agency is one of the more important ones in terms of benefits programs. What kind of commitment is there from the top down in your agency?

Mr. KUSSEROW. Well, of course, our agency has very much benefited by having an inspector general who is a zealot on the subject. So I've been able to raise the awareness of our Secretary and our Assistant Secretary for Management and Budget, and our various agency heads to this area.

Also, I have been willing to expend resources to demonstrate to the Assistant Secretaries—to the Commissioner of Social Security, to the Administrator of the Health Care Financing Administration, to the Assistant Secretary for Human Development Services, to the Assistant Secretary for Health—that indeed we find some of their systems are lacking in proper security measures and are vulnerable. By demonstrating this to them, we have been able to effect a change in attitude.

So, I think we're making a lot of progress in our own Department. But I would be lying to you if I were to say that it's in a satisfactory mode at the present time. We have really got an awfully long way to go.

Mr. GLICKMAN. You recommended that line managers and supervisors receive computer security training. I wonder if you might share with us what you think of the content and purpose of that training, and whether that's happening in any of the agencies now?

Mr. KUSSEROW. We do have it, but I think we should really differentiate between training and indoctrination. First and foremost, we have to indoctrinate our managers. All of our managers that are anyway involved with computerized systems have some responsibility here. It isn't the person down in systems that's supposed to

BEST COPY AVAILABLE

take care of security and everything else. Managers have to make a commitment that they, too, will involve themselves, which means that they either check up and hold their systems managers to a degree of accountability that I don't think exists currently in much of the Federal Government.

So, if we can indoctrinate them on the need, I think that's going a long way.

As far as the training is concerned, knowing what to do is textbook. That's really easy. We're not talking about things that are very complicated here in most cases. We're talking about something that's fairly easy. It's a question of getting commitment out of the managers, and getting commitment out of the people that are one step removed from the systems area, that they indeed have to hold their systems people accountable to good integrity of their computerized systems as well as the data within them.

Mr. GLICKMAN. One final question: How do you feel about NSDD 145, the National Security Directive by NSA?

Mr. KUSSEROW. Well, I would love to be able to see it sometime so I can make a comment. I haven't seen it, and I have not had any input in the process. It may be the most wonderful thing since sliced bread, but I haven't seen it.

Mr. GLICKMAN. Thank you.

That, of course, is one of the problems why we have dealt with this issue and specifically why both my committee and Mr. Brooks' committee have looked at this issue, is because we want to make sure that the civil side of the picture is in the process.

Mr. KUSSEROW. Well, Mr. Chairman, if I had to make a bottom-line statement on where we should be in this area, I think somewhere along the line we're going to have to understand that you just can't assign responsibilities for a system to one individual and have everybody else in a department or agency wash their hands, and say it's not my job, it's somebody else's.

I think what we have to understand, especially with the proliferation of systems the way they are, that every facet of the Government is dependent upon them. As far as I'm concerned, it means that every person in a management position, every employee of the Federal Government has to be made accountable and has to realize that they can't wash their hands or say it's somebody else's job. That's what we heard from GAO this morning, people saying: well, it's not my job, it's somebody else's. Basically, you're not finding the people that would take the responsibility to insure proper system security.

Mr. GLICKMAN. Thank you, Mr. Kusserow.

Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman.

I was curious, Mr. Kusserow, when Mr. Glickman had asked you about the NSDD 145. You said you had not seen it. All parts of that document are not classified. Have you requested it?

Mr. KUSSEROW. Well, we're looking at bits and pieces, but I haven't seen the document in its entirety. We haven't been asked to comment on it. No, I'm sure that we're scheduled for it, but it hasn't progressed to the point where I've looked at it in its entirety. I don't know what the draft looks like.

Mr. LEWIS. So, you don't think——

BEST COPY AVAILABLE

Mr. KUSSEROW. I'm not on any of the task forces on it. I think that it's planned to bring us into the loop somewhere along the line, but I'm not there yet.

Mr. LEWIS. What percentage of computer fraud would you say or would you estimate goes undetected?

Mr. KUSSEROW. I don't know. I would say that there are two problems, Congressman, which are what is detected and what is dealt with or actually reported. I would say that the overwhelming majority of instances where people have engaged in computer fraud or abuse are not detected.

The overwhelming majority of those instances where it is encountered are not addressed or not addressed properly. For example, they find somebody engaging in computer fraud, management as a whole would much prefer to look upon it as computer abuse. If they find a computer abuse problem, management would prefer to find some way in which not to recognize that their system had been diddled with in an improper fashion.

So, we have a tendency to understate those circumstances that are encountered. and we have a tendency not to find the vast majority of the instances. There's plenty of evidence in both the studies to show us that this statement is not out of line.

Mr. LEWIS. You stated that the median number of transactions per crime was eight and that the average duration was 6 months, for an average of $45,000 per crime. I believe you have—yes. And that is over $5,000, actually $5,625 per transaction. What kind of transactions were these, in food stamps, or Medicaid?

Mr. KUSSEROW. We had a lot of different types of transactions. This cut across the benefits programs as well as payroll, as well as contract procurement. It's across the entire spectrum.

Actually, if you want to know the truth, I'm more concerned about those people we didn't find and convict than about the people that we did find and convict. Maybe we might just have a bias here. We got the unlucky ones who were stupid; the smart, lucky ones are still operating. I have some concern about that.

Mr. LEWIS. Were these losses reported? This is a significant amount of money for these types of cases. Were they reported when the checks were diverted, the losses to——

Mr. KUSSEROW. Let me give you an example, Congressman, as to how the system might work and why a lot of lessons come from this as an example. You might have somebody who works as a claims benefits person and all of a sudden they receive notification that someone has died or is no longer eligible for a benefit. It's their responsibility then to delete that individual from the payment system. Let's say instead, though, that individual has the capacity to divert that check and to make it an address change anyway and to a post office box which they control, and that they in turn are able to cash that check or to open another account where they can control the account.

The difficulty is that something is wrong, on a couple of scores, that should have prevented this. One is that when we find that kind of a thing happening, it usually means there's not a good audit trail that is being monitored to show aberrations in the system, or that somebody is doing this kind of thing, or that we could test to see whether anybody is doing it. So, monitoring and

BEST COPY AVAILABLE

audit trails, as referred to by the GAO, are certainly not operating well in that area.

In addition to that, you have to ask the question about segregation of duties. It's a basic principle in any kind of a sensitive financial system that no one person can complete a transaction. You go to the bank, and no bank officer can complete a transaction. It takes two to do it. By segregating those duties, it makes it less likely that somebody can commit a crime. It means that it would take two people to commit a crime.

So, in that example I gave you, it means that not only do they have poor controls to log on, monitor and test the system; but it also means they don't have good segregation of duties if they allow a person to complete a transaction alone.

That seems to me to be the rule when you're dealing with benefit programs: The lack of internal audit controls and the lack of segregation of duties.

Mr. LEWIS. You have been investigating computer fraud for a number of years now. Have any of the findings from your group or groups that you've been involved with resulted in any action that has improved computer security? Or is the situation as bad or worse than it was?

Mr. KUSSEROW. Well, you know, we talked earlier about——

Mr. LEWIS. It's bad, but is it bad or——

Mr. KUSSEROW [continuing]. Well, you're talking about a scale of 5 to 6, on a scale one to 10. I will tell you that there's a lot of folks that haven't even gotten on the screen yet. I mean, they're so far down, they're not even on the screen yet. So, I think in that case any improvement is wonderful. But I will tell you that I think the biggest concern I have is unevenness in the agencies. Some agencies are really doing a marvelous job, and others are doing a terrible job.

I think the efforts that we have been making on the President's Council on Integrity and Efficiency have been to try to work with agencies to develop a baseline of security measures. We have as one of our projects to develop what we think would be the minimal type controls necessary to assure in dissimilar systems some base level of security against diddling. As we point out in the direct testimony, the vast majority of the problems and vulnerabilities are in the areas that are the most easily fixable. It is a question of getting commitment out of the agencies to do that.

So, I think we are making a lot of progress. I am not satisfied with it. I don't want to tell you we're making a lot of progress. I would just as soon have you tell us how bad we're doing so we'll continue to work harder to reduce the vulnerabilities. But we're making progress. We've had conferences involving Assistant Secretaries for Management of all the agencies with the inspectors general. We are really trying to inculcate them with the need to focus their attention on computerized system and to indoctrinate them and to train them so that they can be pushing from the top down.

In some agencies that is really working well, and they're taking it to heart. In other agencies we're not seeing that they have the same degree of enthusiasm. So, it's uneven. One of the frustrations is that it's uneven.

BEST COPY AVAILABLE

It's also frustrating that the systems and their purposes are so different as to make it very difficult to have generic statements as to what is needed in a system and how you go about doing it. And that creates problems. It creates problems because you certainly are going to operate a computerized system that is going to be dealing with AIDS research differently than what you're going to do in another part of our department which relates to benefits programs. They are different systems for different purposes. They both really need to be secured against unlawful intrusions and misuse, but they require different things.

Some problems are line security. Some problems are probably proper access controls with validation and authentication. Some problems are just good physical security. They are all different. It's hard to mandate something across the board without going into a paper processing mode that would on paper look good but in reality be bad. Can we find some way to build better accountability in our managers, to make them realize that they can't pass the buck to somebody else, that they have to be accountable for the system. That's a very tricky thing, too, but I think that's the way it's got to go. How you go about doing it is very difficult to determine.

I think we have a role in it. I think the inspectors general should get out there and maybe have a few public executions, figuratively speaking, among the managers who do not see the commitment in this area and demonstrate to their agencies the consequences of a lack of commitment. Maybe that might help.

Mr. LEWIS. Thank you.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Mr. Packard.

Mr. PACKARD. I am interested in the criminal aspects of it. In your concluding paragraph you indicated that the study shows that one fifth of the perpetrators had former, previous criminal records. That is very interesting, that there very well could be some premeditated efforts to defraud. That being the case, has there been very much filing of charges or prosecuting through the court systems of those that were found guilty?

Mr. KUSSEROW. Everybody that we interviewed in fact did go through the judicial process, and we would say this was a successful outcome, as far as the Government was concerned, that they indeed were prosecuted and justice had prevailed. So, that population group is less disturbing to me than the population group which has not been identified and is operating undetected.

I think the question that we have before us is really twofold. One is, how can we better detect individuals that might be diddling with the system in an improper fashion? More importantly, how can we get on the front-end side of it to prevent them from having the opportunity to do it in the first place, to deny these individuals the opportunity?

But I think your underlying point is, how effectively are we dealing with perpetrators when we encounter and find them? Are we giving them full measure of justice? Or are they somehow slipping through the floorboards of the justice system, and we're not getting them? If that is your point, I will tell you I think that it's very uneven. There has been a lot of concern over the fact that until the last session of Congress we did not have any kind of a bill that

BEST COPY AVAILABLE

would prohibit certain types of activities that would be punishable by Federal law as it relates to computerized systems. We've now begun to have some legislation in that area. In my judgment, it's defective and needs some additional help, but it's a first step at trying to at least have laws specifically addressing individuals who improperly use a computerized system for their own advantage or to the detriment of others.

Another major problem on that line is the agencies. You asked the question of GAO, Mr. Chairman: Were they happy to see you? I have some 20 years of Federal service both in my present capacity and also in the FBI, and I will tell you I have never met anybody yet that appreciated my presence when I came to tell them I was there to help them. They didn't like it. When you did find something wrong, it usually meant that there was an employee that was engaging in nonfeasance, misfeasance, or malfeasance. That is somebody who was lazy, incompetent or on the take. Somewhere up the line in management that was embarrassing. So consequently, they would in many cases take extraordinary steps to try to cover up the fact that there was something naughty going on.

Therefore—and it's consistent with all white collar crime, whether it be bank fraud, securities fraud, or insurance fraud, or fraud in the Federal Government—there's a tendency to grossly understate what the problem is and to deny the fact that there was a crime or to mischaracterize it in a way that would be less embarrassing to agency heads. We've got to get by that.

Mr. PACKARD. Do you have any estimates of those who have been detected, what percentage of reimbursement or restitution you have received in terms of criminal prosecution?

Mr. KUSSEROW. One of the interesting things is that human nature seems to prevail in anything that we do. In the area of investigation or prosecution of criminals, one of the things that is interesting is that investigators only will work as hard as they need to work in order to establish a crime that can be successfully prosecuted. The prosecutors say: Look, I only need about 20 counts to make a case; anything over that is wasted time and energy.

So, what we do have—and I think it's a very serious problem—is the fact that we have a tendency to underinvestigate cases. In looking at the two studies, the first one reviewed agency records to see how they handle them and what they thought the losses were. The other one interviewed the actual perpetrators. What we found was that the perpetrators told us that they took a lot more money than anybody ever found them taking.

The reason for that in large measure is an underinvestigation of the thing, because people say: I'm only going to investigate it enough to get the case prosecuted. And the prosecutor's saying: I only need enough to get this guy; anything over that is wasted energy. The end result is that we do not get the full extent and scope of the crime or the other perpetrators. We've got to change that. That's one of the things we're really pushing on right now.

Mr. PACKARD. I think you're bucking also an inherent difficulty of prosecuting a little old lady or a poor woman, a head of a household with several children. And she's simply trying to make a living and feed her children and often is led to devious ways of

BEST COPY AVAILABLE

doing that. It's pretty hard to vigorously prosecute those kinds of things, I would imagine.

Mr. KUSSEROW. In those instances you're quite right.

Mr. PACKARD. But at any rate, do you have an estimation of the total cost in your Department as a result of computer fraud?

Mr. KUSSEROW. Well, I don't know. I mean, again it's how you define it. If you, as GAO does, talk about the vulnerability of systems to destruction, to waste, to abuse, to fraud, to all those areas, by tightening up in our programs and in the systems that support those programs, there might be as much as a billion dollars in savings.

I will tell you that we're just issuing now, in fact, to the Congress in the next week or a report for the fiscal year 1985 for our Department. In that area as a result of our activities alone is $5 billion that are being collected in terms of fines, savings, and restitution in our Department's programs. So, I think that any statement that has ever been made, except perhaps the ABA, which is anecdotal, about waste and abuse and sometimes fraud in the Government program and systems that support it is probably understated.

Mr. PACKARD. Is your Department, which I am sure uses a considerable amount of computerization, is it pretty well up to date, state of the art use in terms of the technology available for deterrence? I'm sure that the computer industry is constantly looking for ways in their technology of developing computers that are less prone or less able to be vandalized.

Mr. KUSSEROW. I will say this about our Department. We run the whole gamut. We have some of the finest computerized systems in the world, and we have some of the most sophisticated hardware and software that can be purchased anywhere in the world. The reason for that is clear: who's against cancer research? So, you're going to have the best in the area of research in NIH and in the health side of our Department. And we've got some very good computers. We also have some good computers in FDA and some of the other areas of our department.

But I will also have to admit to you that we have had some of the most God-awful primitive hardware and software in the department's programs that are so vulnerable to every aspect that is negative about systems that you could possibly imagine. And they're in some of our most important programs such as Social Security which involve 35 million beneficiaries and shows the importance of getting those systems modernized.

We've got at least six different vintages of computers with hardware and software where vendors and employees to insure their own longevity would use some of the most exotic formats possible so that nobody else could understand them. Then they unfortunately moved on to greener pasture or died off, and nobody else could understand the systems. So, you had manual overrides on everything. And the end result was that we had got nothing but mishmash.

So we've got the best, and we've got the worst. And——

Mr. PACKARD. Let me ask then, is the best in the most critical area as far as protecting public dollars, or is that a concern?

Mr. KUSSEROW. The best is not in the area most vulnerable in terms of dollars. The Social Security Administration has upwards

BEST COPY AVAILABLE

of $200 billion in outlays a year. And that dwarfs anything else in our department. We have had among some of the worst systems. And I think that's why the systems modernization plan there is absolutely critical. That's why we are devoting an inordinate amount of our resources to ensuring that, as they develop the new systems, that they build in the controls and they don't forget, as they usually do. When contractors go in to build new systems, they want to meet deadlines, and tend to make shortcuts. Shortcuts means reductions on the number of controls in the system. We want to make sure they do not cut down on those controls.

Mr. PACKARD. Would time permit one more question, Mr. Chairman?

Mr. GLICKMAN. Sure, go ahead.

Mr. PACKARD. On the other side of that coin, is the industry itself, the computer industry, is it alarmed and responding to the need of better computers and——

Mr. KUSSEROW. I think they're responding to the need, Congressman——

Mr. PACKARD. But——

Mr. KUSSEROW [continuing]. I don't think they're the least bit alarmed. I think they're happy as a pig in clover, the fact that the antiquated systems need replacement. And they're more than happy to give you either hardware or software replacement as needed at the appropriate price.

Mr. PACKARD. But are they implementing technology to the levels that it really is influencing the outcome of——

Mr. KUSSEROW. Well, the technology is here. There's no reason why any system should be lacking in computer security. There's no reason why any system needs to be vulnerable to an inordinate degree to people either improperly intruding upon the technical data within the system or misusing it for their own benefit. The technology is here. It's very simple technology in most cases to correct the problem.

The big problem comes back to how you go about getting management sufficiently committed that they will look at security as being an integral part of any hardware or software purchase, that they will make a commitment to have ongoing testing of the system, and that they will make security a high priority in trying to make the system work and have the continuing attention in that area. If we could only do that, then I think the problem would tend to evaporate, because the technology is here. It's not a question of saying, that we need to put bucks in technology. The technology is here.

Mr. PACKARD. Thank you, Mr. Chairman.

Mr. GLICKMAN. First of all, I want to thank you for your excellent testimony.

Second of all, I want to say that one of the things we are going to ask the GAO to do in any followup is to maybe look further at Social Security, FAA, and a few other systems, which I am sure you will be involved with.

Third of all, I would like to state for the record that one of the problems with the National Security Directive 145 is that HHS is not involved. In fact, if you read the National Telecommunications and Information Systems Security Committee—I think that Mr.

BEST COPY AVAILABLE

Lewis referred to the fact why don't you ask for a copy of the report. The steering group, the civil side of the steering group is the Secretary of Commerce, the Secretary of Transportation, the Secretary of Energy. And then the rest of the group—and the GSA. Other than military groups, we have GSA, FBI, FEMA, and all the rest are military in orientation. So, you're not part of the steering group. I don't know how that steering group got formed——

Mr. KUSSEROW. It's probably a realization that we're only the largest agency in the Federal Government and only represent 38 percent of the Federal budget, and we are probably not worth including in the group.

Mr. GLICKMAN. That's probably what happened.

In any event, I would say that at a minimum that we ought to provide a method internally for your inclusion in whatever process there is.

But I might just point out that this legislation that we are working on right now, this Subcommittee and Government Operations, at least what Government Operations did was to try to modify that directive in some way. I don't know how that legislation will ultimately turn out, but you make an excellent point, that you ought to be involved.

Mr. Brown, do you have any comments right now?

Mr. BROWN. No.

Mr. GLICKMAN. OK. We thank you for your testimony very much. It was very informative testimony.

Mr. KUSSEROW. Thank you, Mr. Chairman.

[The prepared statement of Mr. Kusserow follows:]

BEST COPY AVAILABLE

Statement of Richard P. Kusserow, Inspector General, Department of Health and Human Services

Mr. Chairman, I am Richard P. Kusserow, Inspector General, Department of Health and Human Services. Accompanying me is John I. Molnar, Senior Analyst and Project Leader for our most recent report on computer-related fraud.

Thank you for the opportunity to testify before the subcommittee today on the issue of computer and communications security in the Federal Government. You requested that I discuss the work we have done on computer-related fraud and abuse in the Federal Government for the Computer Security Task Force which I chair for the President's Council on Integrity and Efficiency (PCIE) and to report the specific findings of our most recent study.

The entire Federal Government has become heavily dependent on computers to manage its information. Over 20,000 main frame computerized systems have been identified to date, with additional ones being added almost daily. By 1990, we will have over a half million microcomputers in the Federal Government. This growth in the volume of stored information and number of computers, along with the concomitent increase in persons with access to those systems has made the issue of security a major concern.

In order to gain more information about government computer systems and their vulnerabilities, the PCIE charged me to lead the Computer Security Project. Before reporting on the specific findings of the most recent study, let me briefly summarize some of the work of the Computer Security Project.

- Computer-Related Fraud and Abuse - In June 1983, we reported the findings of a survey of computer-related fraud and abuse among all Federal agencies. This survey identified 103 cases of abuse and 69 fraud cases. Analysis of the survey data indicated that:

BEST COPY AVAILABLE

- Fraud cases primarily involved theft of cash or diversion of assets, usually through input manipulated in benefit or payroll systems. Most abuse cases involved use of computer time for outside business or entertainment.

- Most perpetrators were Federal, nonsupervisory employees. Four out of five of the fraud perpetrators earned $20,000 per year or less. Two-thirds of the fraud perpetrators were functional users of the computer system, rather than data processing personnel.

- Confirmed losses ranged up to $117,383 per case, although actual losses were thought to be higher in many cases.

- Operating personnel found over half of the frauds and over two-thirds of the abuses. More importantly, half of the cases were detected by accident, which was twice the incidence of detection by either controls or audits/reviews.

- EDP Systems Review and Security Analysis - The purpose of this initiative is to increase the effective audit review of automated information systems under development to insure that new systems are installed with adequate internal controls, security features, and audit trails. Through analysis of the roles and responsibilities of key players and documentation necessary throughout a systems life cycle, the project has mapped out the potential audit functions which could be performed. Based on this analysis, an audit guide is being developed under contract and will be published jointly by the PCIE and the National Bureau of Standards, Institute of Computer Science and Technology.

BEST COPY AVAILABLE

- Electronic Media Billing - This study reviewed the process of electronic transmission of health provider claims to Government health care financing programs (i.e., Medicare, Medicaid and Champus). This review found that although formal cost-benefit analysis had not been done, electronic media billing appeared to be a more efficient process than manual billing. However, the review also found that the process contains several vulnerabilities (such as a weak certification process) and needs greater standardization of functions and controls.

- PCIE/PCMI Conference - In June 1984, I co-hosted with Richard H. Shriver, former Treasury Assistant Secretary for Electronic Systems and Information Technology, a one-day conference on computer security for Inspectors General and Assistant Secretaries for Management/Administration. The topics discussed ranged from current management and IG initiatives to private sector techniques available to address computer and communications security problems. One of the recurrent themes was that we can work together to address these problems.

Perpetrator Interviews

With that as background, I will now report on the specific findings of our most recent study - Computer-Related Fraud in Government Agencies: Perpetrators Interviews.

The study was conducted for the President's Council on Integrity and Efficiency (PCIE) as a follow-up to the June 1983 report, "Computer-Related Fraud and Abuse in Government Agencies." The specific objectives for the present study were to identify, locate, and interview the 69 fraud perpetrators from the original

BEST COPY AVAILABLE

DY TO LEARN MORE ABOUT HOW AND WHY THEY COMMITTED THEIR CRIMES, AND TO IDENTIFY COMMON VULNERABILITIES IN GOVERNMENT COMPUTER SYSTEMS.

THE FIRST STEP IN THE STUDY WAS TO IDENTIFY AND LOCATE EACH OF THE PERPETRATORS INVOLVED IN THE ORIGINAL 69 COMPUTER-RELATED FRAUD CASES. BECAUSE MOST OF THE CRIMES HAD BEEN COMMITTED OVER THREE YEARS EARLIER, MUCH OF THE LOCATING INFORMATION WHICH THE AGENCIES HAD WAS NO LONGER CORRECT. WE USED TRADITIONAL FIELD WORK TECHNIQUES TO LOCATE THE PERPETRATORS, AND WE WERE ASSISTED BY TWO OTHER AGENCIES: THE BUREAU OF PRISONS AT THE DEPARTMENT OF JUSTICE LOCATED THOSE WHO WERE IN FEDERAL CORRECTIONAL INSTITUTIONS OR IN PRE-RELEASE PROGRAMS: AND THE DIVISION OF PROBATION IN THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ASSISTED BY LOCATING PERPETRATORS UNDER THE SUPERVISION OF FEDERAL PROBATION OFFICERS.

OF THE 39 PERPETRATORS WE WERE ABLE TO LOCATE, WE INTERVIEWED 29. SINCE MORE CASES OF COMPUTER-RELATED FRAUD HAD OCCURRED IN THE TWO YEARS SINCE THE ORIGINAL STUDY, HOWEVER, WE REQUESTED THAT ALL IGS IDENTIFY ANY SUBSEQUENT CASES. THAT REQUEST YIELDED 18 ADDITIONAL PERPETRATORS OF WHICH WE INTERVIEWED 17: ONE REFUSED.

THUS WE WERE ABLE TO INTERVIEW 46 PERPETRATORS OF COMPUTER-RELATED FRAUD. THESE CASES INVOLVED SEVEN FEDERAL AGENCIES. THE FOLLOWING ANALYSIS OF THE INTERVIEWS IS NOT A DEFINITIVE STATEMENT OF THE EXTENT AND NATURE OF COMPUTER-RELATED FRAUD IN GOVERNMENT AGENCIES, BUT NEW INFORMATION TO ADD TO OUR UNDERSTANDING OF THIS TYPE OF CRIME.

BEST COPY AVAILABLE

PERPETRATORS

IN GENERAL THE COMPUTER FRAUD PERPETRATORS HAD BEEN YOUNG, GOOD EMPLOYEES OF A FEDERAL AGENCY OR A STATE, LOCAL, OR PRIVATE AGENCY ADMINISTERING A FEDERAL PROGRAM. THEIR MEDIAN AGE WAS 30 AND RANGED FROM 20 TO 50. (THE AVERAGE AGE FOR FEDERAL EMPLOYEES IS 40) THREE-QUARTERS HAD SPENT AT LEAST SOME TIME IN COLLEGE. THEY HAD BEEN WITH THEIR RESPECTIVE AGENCIES FOR AN AVERAGE OF 5 YEARS BEFORE THEY COMMITTED THEIR CRIMES. DURING THAT FIVE YEAR PERIOD NEARLY THREE-QUARTERS HAD BEEN PROMOTED, AND TWO-THIRDS REPORTED HAVING RECEIVED AT LEAST AN ABOVE AVERAGE PERFORMANCE RATING. IN FACT, A QUARTER OF THE PERPETRATORS TOLD US THEY HAD RECEIVED PERFORMANCE AWARDS.

NONE OF THE PERPETRATORS IN THIS STUDY, WHO GAINED ACCESS TO THE GOVERNMENT COMPUTER SYSTEM, WERE OUTSIDERS, SUCH AS BENEFICIARIES, CLIENTS, OR HACKERS. ALL OF THE PERPETRATORS WERE AUTHORIZED USERS BECAUSE IT WAS A NECESSARY PART OF THEIR JOB EITHER TO QUERY, ENTER, OR MODIFY DATA IN THE COMPUTER SYSTEM OR TO DIRECT THE OPERATION OF THE COMPUTER SYSTEM.

IT WAS DISCOVERED DURING THE INTERVIEWS, OR THROUGH FBI "RAP" SHEETS, THAT ONE-FIFTH OF THE PERPETRATORS HAD PRIOR CRIMINAL RECORDS AT THE TIME THEY WERE HIRED. SOME HAD EVEN BEEN HIRED UNDER SPECIAL EMPLOYMENT PROGRAMS FOR FORMER FELONS. MOST HAD NOTED THEIR RECORD ON THEIR JOB APPLICATION, BUT A FEW HAD CONCEALED THEIR CRIMINAL RECORDS FROM THE AGENCIES THAT HIRED THEM. PERPETRATORS WITH FORMER CRIMINAL RECORDS WERE MORE LIKELY TO BE STATE OR LOCAL EMPLOYEES THAN FEDERAL EMPLOYEES AND WERE MORE LIKELY TO COMMIT THEIR CRIME DURING THEIR FIRST YEAR OF EMPLOYMENT THAN THOSE WITHOUT A RECORD.

BEST COPY AVAILABLE

Their Jobs

Their jobs gave perpetrators the access they needed to commit their crime. Three-quarters of the perpetrators worked in benefit programs and were in a position to cause those funds to be issued. They held a wide variety of positions ranging from senior program managers to clerks. The most common type of position was caseworker. These are people whose primary job was to make eligibility or payment decisions on entitlement programs. Other common position types were computer support or technical personnel such as data entry technicians. One-fourth of all the perpetrators were in supervisory positions.

Not all of the perpetrators had direct access to the computer system. Forty percent of the perpetrators' jobs, primarily caseworkers, called for them to create input documents which would be loaded into the computer system by data entry technicians. Consequently, while these perpetrators had to have an indepth understanding of the computer system, they did not have to sit at a computer terminal to commit their crime.

The Crimes

Most perpetrators caused negotiable financial instruments to be issued by manipulating data input to the computer system. The perpetrators used three different schemes to accomplish this. Most frequently, they modified existing cases in ongoing payment programs, such as the Unemployment Insurance, Food Stamp, or Social Security programs or a payroll system. Typical modifications were to simply change the address to which the payments were sent.

BEST COPY AVAILABLE

THE SECOND MOST COMMON SCHEME WAS TO CREATE FALSE CLAIMS IN ONE-TIME PAYMENT SYSTEMS. TYPICALLY, THE PERPETRATOR AUTHORIZED PAYMENTS FOR BOGUS BILLS, SUCH AS THOSE FOR PAYMENT OF A PURCHASE ORDER, OR FOR REIMBURSEMENT TO BENEFICIARIES OR PROVIDERS FOR MEDICAL SERVICES. THE PAYMENTS WERE USUALLY SENT TO FRIENDS OF THE PERPETRATOR.

THE THIRD AND MOST DIFFICULT OF THE SCHEMES WAS TO CREATE FALSE CASES IN ONGOING PAYMENT PROGRAMS. THIS WAS DIFFICULT BECAUSE THE PERPETRATOR HAD TO ESTABLISH ELIGIBILITY FOR THE BOGUS CASE. TO DO THIS, THEY EITHER USED THE IDENTITY OF A CO-CONSPIRATOR OR WENT THROUGH THE PROCESS OF CREATING FALSE IDENTITIES.

TYPICAL OF WHITE COLLAR CRIMES, MOST PERPETRATORS TOOK STEPS TO COVER UP THEIR CRIMES. MANY OF THOSE WHOSE SCHEMES INVOLVED ON-GOING PAYMENTS TERMINATED THEIR BOGUS CASES AFTER A FEW MONTHS TO REDUCE THE LIKELIHOOD OF DETECTION BY A QUALITY CONTROL AUDIT OR A RECERTIFICATION. ABOUT 40 PERCENT OF THE PERPETRATORS REPORTED THAT THEY DESTROYED THE "HARDCOPY" EVIDENCE OF THEIR CRIME, AND ANOTHER 10 PERCENT SAID THEY DELETED THE RECORD OF THEIR ILLEGAL TRANSACTIONS FROM THE COMPUTER SYSTEM.

THREE-FOURTHS OF THE PERPETRATORS USED CO-CONSPIRATORS IN THE COMMISSION OF THEIR CRIMES. THE CO-CONSPIRATORS SERVED TWO SPECIFIC PURPOSES: 1) CO-CONSPIRATORS WHO WERE OUTSIDE OF THE AGENCY WERE USUALLY USED FOR THEIR IDENTIFICATION, AND TO RECEIVE AND CASH CHECKS; AND 2) FELLOW EMPLOYEES WHO WERE USED FREQUENTLY TO BYPASS CONTROLS SUCH AS SEPARATION OF DUTIES.

WHILE THE EXTENT OF THE PERPETRATORS' CRIMES VARIED GREATLY, DATA ON THEIR AVERAGE FREQUENCY, DURATION, AND DOLLAR AMOUNTS PROVIDE SOME PERSPECTIVE. AGENCIES LOST AN AVERAGE $45,000 PER CRIME IN THESE CASES. THE AVERAGE DURATION OF CRIMINAL ACTIVITY WAS ABOUT SIX MONTHS. THE NUMBER OF ILLEGAL COMPUTER TRANSACTIONS PER CRIME RANGED FROM ONE TO 200, ALTHOUGH THE MEDIAN FREQUENCY WAS ONLY EIGHT.

BEST COPY AVAILABLE

The Motives

Most perpetrators reported that they stole because of situational stresses. These stresses fell into two categories. About 60 percent of the perpetrators said that they stole money because of a specific problem they were facing such as medical bills, over-indebtedness, imminent eviction, or loss of spousal income. Another 10 percent attributed their stress to being disgruntled. Some of these employees were mad at the organization, while others were seeking revenge against an immediate supervisor.

Those who did not steal because of stress, stole because a vulnerability in the system was present, and they could not resist the temptation. In some cases a specific event, such as funds being returned to the office, or the accidental discovery of a vulnerable procedure in the system, triggered the crime. Other perpetrators were bored or had free time and would play "beat the system" at the terminal until they won the game.

The Opportunity

About half of the perpetrators reported that they did not even think about the consequences of their actions, and most of the others assessed the risks of being caught as minimal. A number of factors led to these attitudes among the perpetrators.

Most perpetrators felt that controls and system security were weak. In fact, some of the systems did not have controls or audit trails. When access controls, screens, and separation of duties were designed into computer systems, perpetrators saw that poor implementation at the user level often undermined security. Access controls were often simplistic, or were bypassed in daily

BEST COPY AVAILABLE

PRACTICE IN THE INTEREST OF PRODUCTIVITY. EDITS AND SCREENS IN THE SYSTEM WERE WELL KNOWN TO ALL SYSTEM USERS, AND THE PERPETRATORS USUALLY SIMPLY AVOIDED THEM. SEPARATION OF DUTIES COULD BE UNDERMINED WHEN, DUE TO STAFFING CHANGES, A PERSON WAS TRAINED IN BOTH INPUT AND OUTPUT DUTIES, OR SIMPLY WHEN TERMINALS WERE LEFT UNATTENDED AFTER BEING BROUGHT ON-LINE.

ANOTHER FACTOR THAT INFLUENCED THE PERPETRATORS WAS THEIR PERCEPTION THAT THE SYSTEM WAS VULNERABLE. TWO-THIRDS REPORTED THAT THEY WERE AWARE OF OTHER CRIMES "LIKE THEIRS." THEY WERE EQUALLY DIVIDED BETWEEN THOSE WHO SAID THEY KNEW OF SPECIFIC CRIMES, AND THOSE WHO SAID THEY HAD HEARD OF SUCH CRIMES. IN THE WAKE OF THESE COMPUTER CRIMES, IT WAS COMMON FOR THE MODUS OPERANDI OF THE PERPETRATOR TO BE SPREAD BY RUMOR.

SIGNIFICANTLY, THE PERPETRATORS FREQUENTLY VOLUNTEERED THAT THEY WERE NOT BEING WATCHED. THEY REPORTED THAT SUPERVISION WAS WEAK FOR TWO REASONS. FIRST, SOME PERPETRATORS REPORTED THAT SUPERVISORS DID NOT REVIEW THEIR WORK, EITHER BECAUSE THEY WERE TRUSTED EMPLOYEES, BECAUSE THE SUPERVISOR WAS TOO OVERLOADED TO REVIEW EVERYTHING, OR SIMPLY BECAUSE WORK GENERALLY WAS NOT REVIEWED. THE SECOND FORM OF WEAK SUPERVISION WAS OF A MORE TECHNICAL NATURE. SOME PERPETRATORS REPORTED THAT THEIR SUPERVISORS DID NOT KNOW HOW THE JOBS AT THE COMPUTER TERMINAL WERE PERFORMED. SUPERVISORS OFTEN CAME UP THROUGH THE PROGRAM WHEN THE JOB HAD BEEN MANUAL AND HAD NEVER LEARNED HOW THE JOB IS DONE ON THE AUTOMATED SYSTEM. ACCORDINGLY, PERPETRATORS WERE ABLE TO TAKE ADVANTAGE OF SUCH SUPERVISORY NAIVETE.

PERPETRATOR SUGGESTIONS

WE ASKED EACH PERPETRATOR HOW THEY WOULD IMPROVE COMPUTER SECURITY AT THE WORK SITE. THEY OFFERED A NUMBER OF COMMON,

BEST COPY AVAILABLE

USABLE SUGGESTIONS. FOR EXAMPLE, THEY SUGGESTED THAT SUPERVISORS RANDOMLY PULL CASE FILES AND CALL THE BENEFICIARIES TO VERIFY CASES OR ROTATE CASELOADS PERIODICALLY SO THAT A WORKER DOES NOT HAVE EXCLUSIVE CONTROL OF A PROVIDER, CONTRACTOR, OR BENEFICIARY FILE. THEY RECOMMENDED CREATING AUDIT TRAILS SO THAT THE WORKER WHO AUTHORIZES A PAYMENT AND ENTERS THE TRANSACTION INTO THE SYSTEM IS IDENTIFIED WITH THE CASE FILE IN THE SYSTEM. SOME ALSO RECOMMENDED USING INDIVIDUAL IDENTIFICATION NUMBERS TO LIMIT ACCESS WITHIN THE COMPUTER TO THE WORKERS' SPECIFIC RESPONSIBILITIES.

Study Recommendations

BASED UPON THE DATA CONTAINED IN THIS AND THE EARLIER REPORT, WE MADE A NUMBER OF SPECIFIC RECOMMENDATIONS TO PCIE.

ONLY EIGHT OF THE 46 PERPETRATORS HAD BEEN DEBRIEFED TO IDENTIFY SYSTEM VULNERABILITIES. COMPUTER FRAUD PERPETRATORS SHOULD BE DEBRIEFED ON A ROUTINE BASIS NOT ONLY TO IDENTIFY SPECIFIC SYSTEM VULNERABILITIES, BUT ALSO TO ADD TO OUR GENERAL KNOWLEDGE OF COMPUTER-RELATED CRIME AND TO INSURE THAT NO CO-CONSPIRATOR IS UNDETECTED. WE HAVE IMPLEMENTED THIS PROCESS IN MY OFFICE.

THESE CRIMES INDICATE A CLEAR NEED TO STRENGTHEN CONTROLS IN THE VICTIMIZED SYSTEMS.

- EXISTING COMPUTER SECURITY NEEDS TO BE REVIEWED AND MONITORED TO ASSURE PROPER IMPLEMENTATION.

- BETTER AUDIT TRAILS NEED TO BE BUILT INTO OUR SYSTEMS TO ASSURE ACCOUNTABILITY.

- USER ACCESS MUST BE LIMITED WITHIN THE SYSTEM TO SPECIFIC JOB RESPONSIBILITIES.

BEST COPY AVAILABLE

GIVEN THAT HALF OF THE PERPETRATORS WORKED FOR STATE AND LOCAL GRANTEES OR PRIVATE CONTRACTORS, WE MUST REEVALUATE OUR GUIDANCE TO SUCH AGENCIES TO ASSURE THAT COMMITMENT TO SECURITY EXISTS IN THESE SYSTEMS. WE NEED TO ASSURE THAT PROGRAM MANAGERS AND LINE SUPERVISORS ARE KNOWLEDGEABLE AND COMMITTED TO COMPUTER SECURITY BY PROVIDING THEM WITH TRAINING. FINALLY, GIVEN THE FINDING THAT OVER ONE-FIFTH OF THE PERPETRATORS HAD CRIMINAL RECORDS WHEN HIRED, WE MUST ASSESS THE EFFECTIVENESS OF OUR PERSONNEL SECURITY PROGRAMS WITH REGARD TO POSITIONS WHICH HAVE ACCESS TO AUTOMATED FINANCIAL OR PAYMENT SYSTEMS.

MR. CHAIRMAN, I THANK YOU FOR THE OPPORTUNITY TO OUTLINE OUR ACTIVITIES AND TO REPORT ON THE PERPETRATOR INTERVIEW STUDY. THIS CONCLUDES MY PREPARED STATEMENT. I AM AVAILABLE TO ANSWER ANY QUESTIONS YOU MAY HAVE.

BEST COPY AVAILABLE

Mr. GLICKMAN. The next witnesses are representatives from the Department of Agriculture. Mr. Robert Beuley is the Deputy Inspector General, accompanied by Mr. Donn Adkisson, Assistant Inspector General for Audit.

Mr. Beuley, it's a pleasure to have you here. As I have told the other witnesses, your entire statement will appear in the record. So, if you want to summarize it to try to expedite the process, give us more time for questions that way.

STATEMENT OF ROBERT W. BEULEY, DEPUTY INSPECTOR GENERAL, U.S. DEPARTMENT OF AGRICULTURE, ACCOMPANIED BY DONN E. ADKISSON, ASSISTANT INSPECTOR GENERAL FOR AUDIT

Mr. BEULEY. Thank you, Mr. Chairman.

Mr. Chairman and members of the committee, thank you for the invitation to appear before you today to discuss the Office of Inspector General audit of the security over non-Federal computer systems.

I would like to highlight a few points in my statement.

The OIG audit centered in the major programs of the Food and Nutrition Service that are administered by State and local agencies. In fiscal year 1984 the Food and Nutrition Service made about $12 billion in benefits available to the State agencies for disbursements to individual recipients.

Mr. GLICKMAN. Excuse me. We're talking substantially about the Food Stamp Program, aren't we?

Mr. BEULEY. Yes, sir, and the Women, Infants, and Children Program.

Our office reviewed 13 non-Federal computer systems which processed about 20 percent of the FNS-funded benefits disbursed in 1984, to an average of over 5 million program participants monthly. We found security weaknesses in all 13 systems. Some of the more serious weaknesses concern inadequate controls over physical security, thus permitting unauthorized access to computer hardware, and inadequate software controls which would enable persons to improperly manipulate data and payments.

While we did not attempt unauthorized access of these systems, our analysis of the inherent risk involved made it apparent that the area is highly vulnerable to fraud, waste and abuse.

I will categorize each security control area in which the major weaknesses were prevalent. The State agencies audited have initiated corrective action and we will direct our followup efforts in the future to review the adequacy of these actions.

The first area is organizational controls. The weaknesses in the organizational controls included a lack of security awareness training, risk analyses, security plans, separation of duties, and security clearances, much as what GAO just presented to you relating to the Federal systems. As a matter of fact, at one large statewide agency, background checks prescribed for newly hired personnel did not include screening through the State's own welfare fraud agency. Our audit identified two current employees that had entered guilty pleas to welfare fraud offenses.

BEST COPY AVAILABLE

We found that four States did not require background investigations. And two other States' prescribed checks were inadequate, which ties in a lot with what Mr. Kusserow just talked to you about.

The second area is physical security controls. The weaknesses included terminals which had the capability of updating files were accessible to unauthorized individuals, inadequate password controls, inadequate physical security, inadequate security or management of the tape libraries, and safety and fire hazards.

The third area is the input/output controls and the system software controls. They were inadequate in most instances. Problems found included system accesses not logged, terminals not shut down after a set number of invalid attempts were made on the terminals, no passwords, or passwords not suppressed on reports and printouts. So, anyone that went by could review the passwords and pick it up.

The fourth area deals with contractor systems processing grantee payments.

One of the 13 systems included in our audit was a contractor-developed system. We noted that the contract for ADP services did not include sufficient security requirements to ensure protection of data and payments. Also, the contract did not specify the authorities of the Department and the General Accounting Office to review the system operations, programming and related activities.

The fifth area was the Food and Nutrition Service oversight of the systems.

FNS needed to improve its monitoring and oversight of the ADP security. From fiscal year 1983 through midfiscal year 1985, the 6 FNS regional offices that we audited made only 10 reviews out of a universe of some 86 potential systems to review, of the security matters ranging from 4 by 1 office and none by 2 other offices. In addition, the documentation was lacking to support these reviews in most cases, and the reviews generally did not disclose the problems similar to the ones we disclose in our audit.

FNS has not delineated minimum security requirements for its grantees. FNS's position is that the Office of Management and Budget circulars and Federal regulations do not provide that the Federal ADP security requirements apply to non-Federal systems. FNS also maintains, and we also agree, that the issue cross-cuts Federal agencies and programs, and the optimum solution would be a Federal ADP security regulation which would apply to all Federal programs. It is also our opinion that the State agencies are ultimately responsible for the implementation of adequate ADP controls over their systems. However, it's incumbent upon the Food and Nutrition Service to monitor the accuracy of the implementation, particularly in their area.

FNS has agreed to initiate several actions in line with our recommendations to strengthen the ADP security in the non-Federal systems. They plan to expedite written notification to all the other State agencies and pointing out the importance of controls and the problems we found, develop initial guidelines extracted from the Federal information processing standards, and they will work toward incorporating these provisions in regulations, streamlining its monitoring of the oversight of the ADP security to the existing

BEST COPY AVAILABLE

systems, and they also said they will work with the Department of Agriculture's central guidance agencies and HHS and the Office of Management and Budget to promulgate recognized ADP security standards to all non-Federal entities which process Federal data.

Mr. Chairman, that concludes my highlights. I would answer any questions you have.

Mr. GLICKMAN. Thank you very much, Mr. Beuley.

I think the essence of your statement is that you're an agency that is responsible for the administration of the expenditure of billions of Federal dollars, but it is managed by the States. In terms of the actual day-to-day administration of the programs are done, in the Food Stamp Program——

Mr. BEULEY. In the Food Stamp Program——

Mr. GLICKMAN [continuing]. By the States. WIC is, I think, done federally, is it? Or is WIC done by the States?

Mr. ADKISSON. It's done by the States.

Mr. GLICKMAN. As well.

So, you say FNS's position is that OMB circulars and Federal regulations do not provide that Federal ADP security requirements apply to non-Federal systems, which, in effect, means that there is no regulatory requirement or other forms of requirements whereby you can effectively control computer security done by State systems?

Mr. BEULEY. That's correct. They have a broad authority to require in the agreements that there be adequate security, but no provisions to state what the minimum standards should be that the States must follow.

Mr. GLICKMAN. So again we have a problem of Federal dollars being expended, but you would not have the control over the computer systems like you would if you were talking about—you being HHS, and you were talking about the Social Security system.

Mr. BEULEY. That's right.

Mr. GLICKMAN. I am just wondering, off the top of your head, do you know, what other Federal programs operate like this, with the States administering Federal dollars? Is Medicaid——

Mr. BEULEY. Well, Medicaid, I believe, is administered mainly by the States, and the ADC payments.

Mr. GLICKMAN. So, other than Social Security, the bulk of our income transfer programs are administered by the States?

Mr. BEULEY. That's correct.

Mr. GLICKMAN. And the Federal Government has basically no compelling requirements or no way to require the States right now to get their computer systems up to snuff in terms of security measures then?

Mr. BEULEY. They do not have minimum essential standards that each State has to follow in the computer security area.

Mr. GLICKMAN. Are there any legal impediments that would prevent the Federal Government from imposing those kinds of requirements?

Mr. BEULEY. I don't know. I would think, that if the States wanted the Food and Nutrition Service money, and FNS wanted certain controls since they have the oversight responsibility, then FNS could require certain minimum standards. I am not aware of any legal impediments.

BEST COPY AVAILABLE

Mr. GLICKMAN. No reason why the Department of Agriculture couldn't, when they negotiate the program administration with the States couldn't require those kind of minimum standards then. Is that correct?

Mr. BEULEY. As a matter of fact, I said they plan to do more in that area, but FNS believes that it's not just a unique FNS problem; it's a Governmentwide problem. And they also plan to work with the Office of Management and Budget to try to get some Governmentwide standards. So, it's not just FNS putting a requirement on the State. If the States are also receiving money from HHS or Education, they should also meet those minimum standards, particularly if the States have an integrated computer system.

Mr. GLICKMAN. I added language to the food stamp bill largely in response to the fact that my staff had been talking to you about these issues, which tries to at least focus the Department of Agriculture's attention to this problem, the problem of benefits being administered by the States. But as you suggest, it's a systemwide problem.

Do you believe that the problem is more acute, the problems of computer security are more acute in circumstances where the benefits are being administered by the States than if the benefits were being administered by the Federal agencies?

Mr. BEULEY. It's hard to judge that one. I guess the only thing I can judge by is what GAO just presented on their problems with the Federal agencies and their estimation of where the Federal agencies stand. Based on the 13 non-Federals that we looked at, the situation was worse as far as security in those 13 non-Federal systems are concerned.

Mr. GLICKMAN. Going back to the GAO's general comments, you heard their overall assessment of computer security in Federal agencies as well as its comments on specific weaknesses. I wonder if you might have any general comments on the GAO's report this morning.

Mr. BEULEY. Well, based on my background knowledge, I would say that they're on target on the types of problems and the impacts of those problems and the lack of attention or training, particularly with the new emphasis bringing everyone up to state of the art. With the micros and the minicomputers expanded use, it makes it even more important that the awareness and the training gets down even further into organizations because you're beginning to take your control system and spread it out to more and more people.

Mr. GLICKMAN. FNS seems to have agreed with all of your recommendations. Does the agency have the expertise to carry out a rigorous computer security program?

Mr. BEULEY. I believe they will need some additional expertise, but I would imagine you would probably need to ask FNS after they lay out the plan. I would imagine from the reviews that they did not do that. FNS needs some additional help and expertise.

Mr. GLICKMAN. So they could use computer training assistance by, let's say, the Bureau of Standards or perhaps the private sector as well?

BEST COPY AVAILABLE

Mr. BEULEY. Right. There are a lot of courses available out there right now.

Mr. GLICKMAN. The previous witness, Mr. Kusserow, testified that he was a zealot on the issue of computer security. How would you characterize the inspector general's office in the Department of Agriculture in this area?

Mr. BEULEY. Well, I would say that we are close. As far as zealots go, we are in that category. As a matter of fact, we have established a separate group for financial management systems with ADP auditors to concentrate strictly on financial management systems and ADP controls within Agriculture on that. We have added computer specialists and ADP auditors in all our regions, and we've expanded by providing microcomputers and microcomputer training to get up to the state of the art not only in the auditing but to use the computer in our audits and investigations.

Mr. GLICKMAN. One final question: Mr. Kusserow referred to some specific interviewing that he had done with respect to violators. Did you do any of that? Do you have any idea what the amount of loss might be in the food stamp system every year, just taking that one system, with respect to breaches of the security of computers?

Mr. BEULEY. I will ask Mr. Adkisson. I have only been at Agriculture for 6 weeks.

Mr. ADKISSON. We did not do any of the perpetrator interviews that Mr. Kusserow did. He took the lead and did all those interviews. In Agriculture we did not do any of those perpetrator interviews.

As far as computer fraud, it's hard to define precisely, because everyone has their own definition of what computer fraud is.

Mr. GLICKMAN. But you can define losses. I mean, a lot of the things that have been—that he talked about at HHS are applicable to some of the benefit programs that you administer. Do you have any way to quantify your losses with respect to that kind of fraud, as opposed to the more normal kind of fraud that may deal with people getting more benefits than they're entitled to?

Mr. ADKISSON. I don't have those figures with me. I think we could probably put together some maybe ballpark figure as to maybe 5 to 10 percent or 10 percent or 20 percent. We have done a number of matching of different computer lists. And we've had a high rate of success with work with Dick Kusserow, the Department of Labor and some of the others, and have matched participation in the various programs against various files. And we've come out with a very high rate. Some of those are insider crimes, case workers, multiple case worker fraud, everything Mr. Kusseron said we have in Agriculture——

Mr. GLICKMAN. We would appreciate receiving information relevant to this because it's useful in terms of the overall issue, which has to do with computer training at all levels of your employment.

Mr. BEULEY. I think there's one thing. You have to make two distinctions when you're talking about this broad area of computer crime. On the one side, which is a lot of the cases that Mr. Kusserow dealt with, are people that develop false documents, false bills. A lot of this fraud dealt with input before it got into the computer. And you still have this type of vulnerability out there.

BEST COPY AVAILABLE

The other, more technical type fraud is actually getting into the computer program, unauthorized access, playing with the computers, and developing traps in the programs. This is a much more technical area. I don't think, in the whole IG community, that we have a lot of cases of this type.

Now, in the first category, it's critical that the basic essential controls like passwords and physical security are adequate. But the more critical element is, what kind of management information systems being developed that will try to match and merge and look for things that look out of the ordinary to give you an exception listing to pursue those types of potential errors and abuses

There's also a problem with developing good management information systems and exception reports that will help you to detect abnormalities that you need to pursue.

Mr. GLICKMAN. OK. Thank you.

Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman.

Mr. Beuley, you stated that State agencies that you have audited have initiated corrective actions. Could you be more specific as to what actions have been taken?

Mr. BEULEY. Donn, can you elaborate on this?

Mr. ADKISSON. Yes.

Mr. LEWIS. And also, how long ago did you make this audit?

Mr. ADKISSON. OK. The audit started about a year ago. We just completed and released the report last Friday, I believe. So, it took us about a year to do those 13 audits.

The State agencies, by and large, were very responsive when we pointed out weaknesses in their security. For example, in one case we found where the passwords had not been changed for over 10 years in one of the units. They immediately saw that this was a severe weakness, and they changed all the passwords immediately. Things like that were taken care of as soon as we brought it to their attention.

Mr. BEULEY. In other words, they started to change programs to suppress the passwords that came out on the listings, and things of that nature. Other are going to take them a little longer to do. What we plan to do is go back and do a followup audit to find out how they're coming along on these items.

But the more important thing is that we told the Food and Nutrition Service to get out a letter which they are developing right now to report the problems to all the other State agencies that we did not get to and tell them to take a look at their own operation and, if they have these vulnerabilities, to quickly fix them.

Mr. LEWIS. Who pays for the waste or the fraud in the system, the State or the Federal Government?

Mr. BEULEY. Well, I would imagine it's a matching situation. So, I guess the States would share in it, because they are matching administrative cost. The direct benefits would be mostly paid by the Federal Government, but the processing costs would be shared.

Mr. LEWIS. What incentive does the State agency have to avoid wasting Federal funds?

Mr. BEULEY. Well, a lot of these systems are also not just for Food and Nutrition Service programs. They run their own systems on it, so many of them have the incentive that their own money

BEST COPY AVAILABLE

needs to be protected as well as the Federal agencies. I think this is the basic incentive.

If they've got a program that's unique and just running the food and nutrition programs I guess the incentive there is that the Department of Agriculture, if they do not correct it, can take action to hold back some money. And that becomes a pretty good incentive to straighten out your problems.

Mr. LEWIS. Do you know if this has been done at all?

Mr. BEULEY. I don't know whether it has been done in the past or not.

Mr. ADKISSON. It has not been done on computer problems. It's been done for general mismanagement of the programs. They have a regular sanction process.

Mr. LEWIS. Why wouldn't you do it for computers?

Mr. ADKISSON. I think, for one reason, is that we have not demonstrated sufficiently a loss that the Food and Nutrition Service could then take action against a specific area, a particular agency.

Mr. BEULEY. Part of the problem is because of the security weaknesses. There is not a good audit trail. For example, they did not maintain computer logs so you know whether there has been an unauthorized access in the system. In one agency they only kept their log sheets for 2 days, so there was a lack of a good audit trail to go back and to prove what has happened.

Mr. LEWIS. Do you believe that the computer systems in the State agencies are worse than the Federal systems as far as security?

Mr. BEULEY. Based on GAO's current representation, I would say yes, at least based on the 13 we looked at.

Mr. LEWIS. Thank you, Mr. Chairman.

Thank you, gentlemen.

Mr. GLICKMAN. Thank you.

Mr. Brown.

Mr. BROWN. Just one question I wanted to ask that may have been covered previously and, if it has, why I apologize. Do we have for the Federal Government acceptable standards as to what constitutes the proper security procedure within a system, within a computer system itself? In other words, for any given level of risk from breaching security, are there appropriate levels or standards that we say these should apply in order to have the necessary probability that we're not going to have breaches of security and so on?

Mr. BEULEY. I would say that I think the Federal information processing standards do provide adequate guidance dealing with all of these areas as far as security passwords, and that type of thing. Now, in actual implementation it depends a degree on how far an agency goes. There are some software control packages that you can put in your systems that will further protect them and make it very difficult to get into. They are available and it's up to the agency in that particular vulnerability of that system whether they want to use that or another from of security controls.

But the Federal standards recognize and lay out the types of things you can do. And I think it's a good baseline document. I am sure they continually go through improvements. But I think, if everybody followed the Federal processing standards down the line,

BEST COPY AVAILABLE

you would eliminate a lot of the vulnerabilities that you have right now.

Mr. BROWN. But there is no uniform application of those, no requirement that they be——

Mr. BEULEY. No. It's a standard, it's a guideline. It's not required that you go follow it A to Z.

Mr. BROWN. I have nothing further.

Mr. GLICKMAN. Thank you.

I appreciate it, Mr. Beuley, your being here.

I wonder if Mr. Franklin, did you hear Mr. Brown's question? I wonder if—he asked if there are any Federal guidelines that agencies would have available to them on, you know, computer security standards right now. I wonder if you might be able to comment. Are there any specific guidelines out by anybody that are applicable?

Mr. FRANKLIN. There aren't any that are applicable across Government now. The National Bureau of Standards does have some standards, however, some of them are labelled or Federal information processing standards; but they are actually guidelines. For example, FIPS 31,[1] which basically deals with physical security, is a standard. The other documents like 64 are guidelines. There is no single comprehensive set of those publications that are put out to Federal agencies as being binding on the Federal agencies. That is in the discretion of the agency head whether or not he uses all or any portion of the guidelines.

And it's also at the discretion of the head of the agency as to what kind of program he puts together to administer it. So, like we said in our testimony, there needs to be a catalyst. And there needs to be some amount of consistency in putting together security programs and the various components of those programs like a risk management component of your program, the training component of your program, et cetera.

Mr. GLICKMAN. OK. Thank you very much.

Thank you, Mr. Beuley.

[The prepared statement of Mr. Beuley follows:]

[1] Mr. Franklin meant to refer to FIPS PUB 46 "Data Encryption Standard."

55-930 0 - 86 - 4

BEST COPY AVAILABLE

PREPARED STATEMENT OF
ROBERT W. BEULEY, DEPUTY INSPECTOR GENERAL
U.S. DEPARTMENT OF AGRICULTURE
BEFORE THE HOUSE SCIENCE AND TECHNOLOGY SUBCOMMITTEE
ON TRANSPORTATION, AVIATION AND MATERIALS

MR. CHAIRMAN, AND MEMBERS OF THE COMMITTEE, THANK YOU FOR THE INVITATION TO APPEAR BEFORE YOU TODAY TO DISCUSS THE OFFICE OF INSPECTOR GENERAL AUDIT OF THE SECURITY OVER NON-FEDERAL COMPUTER SYSTEMS.

AUDIT OF NON-FEDERAL COMPUTER SYSTEMS

OIG'S AUDIT CENTERED ON THE MAJOR PROGRAMS OF THE FOOD AND NUTRITION SERVICE (FNS) THAT ARE ADMINISTERED BY STATE (AND LOCAL) AGENCIES. IN FISCAL YEAR 1984, FNS MADE ABOUT $12 BILLION IN BENEFITS AVAILABLE TO THE STATE AGENCIES FOR DISBURSEMENT TO INDIVIDUAL RECIPIENTS. OIG REVIEWED 13 NON-FEDERAL COMPUTER SYSTEMS WHICH PROCESSED ABOUT 20 PERCENT OF FNS-FUNDED BENEFITS DISBURSED IN FY 1984 TO AN AVERAGE OF OVER 5 MILLION PROGRAM PARTICIPANTS MONTHLY. WE FOUND SECURITY WEAKNESSES IN ALL 13 SYSTEMS; SOME OF THE MORE SERIOUS WEAKNESSES CONCERNED INADEQUATE CONTROLS OVER PHYSICAL SECURITY, THUS PERMITTING UNRESTRICTED ACCESS TO THE COMPUTER HARDWARE, AND INADEQUATE SOFTWARE CONTROLS WHICH WOULD ENABLE PERSONS TO IMPROPERLY MANIPULATE DATA AND PAYMENTS. WHILE WE DID NOT ATTEMPT UNAUTHORIZED ACCESSES OF THESE SYSTEMS, OUR ANALYSIS OF THE INHERENT RISKS INVOLVED (LARGE SUMS OF MONEY; EXISTENCE OF THIRD PARTY BENEFICIARIES; PAYMENT OF ENTITLEMENT MONIES; DEGREE OF DECENTRALIZATION) MAKE IT APPARENT THAT THE AREA IS HIGHLY VULNERABLE TO FRAUD, WASTE, OR ABUSE.

BEST COPY AVAILABLE

I WILL CATEGORIZE EACH SECURITY CONTROL AREA IN WHICH MAJOR WEAKNESSES WERE PREVALENT. THE STATE AGENCIES AUDITED HAVE INITIATED CORRECTIVE ACTION AND WE WILL DIRECT OUR FOLLOWUP TO THE ADEQUACY OF THESE ACTIONS.

ORGANIZATIONAL CONTROLS

WEAKNESSES IN ORGANIZATIONAL CONTROLS INCLUDE A LACK OF SECURITY AWARENESS TRAINING, RISK ANALYSIS, SECURITY PLANS, SEPARATION OF DUTIES, AND SECURITY CLEARANCES. Some examples are:

- For one Statewide system, the State Agency had not implemented an overall ADP security program. The State Agency had not: designated a security officer, developed a security plan, conducted risk analyses, developed contingency plans, made security reviews, or provided security awareness training. The State Agency relied solely on user identification numbers and passwords to protect the system and files. Assurance of reasonable security over this system was lessened due to the method used to assign passwords; three individuals knew all the passwords, and each user's supervisor was also privy to the passwords assigned. The system also had no means of detecting or tracking unauthorized accesses; further, any terminal in the State could be used to manipulate the data files maintained on the system.

- At another large Statewide system, background checks prescribed for newly hired personnel did not include a screening through the State's own

BEST COPY AVAILABLE

welfare fraud agency. Our audit identified two current employees that had entered guilty pleas to welfare fraud offenses. We found that four States did not require background investigations and two other States' prescribed checks were inadequate.

- Six States and one county included in our review had no disaster recovery plans. Although the county had arranged for a back-up site, it had not developed procedures to process critical data. ADP officials stated the county would probably revert to a manual system should the computer go down. At a State site which processes about $100 million annually in Food Stamp benefits, an internal review report acknowledged that the "loss of computer capability for any prolonged period of time would put (the) State Government out of business." Nonetheless, they had no back-up plan and had not designated a backup site.

PHYSICAL SECURITY CONTROLS

WEAKNESSES INCLUDED: TERMINALS WHICH HAD THE CAPABILITY OF UPDATING FILES WERE ACCESSIBLE TO UNAUTHORIZED INDIVIDUALS, INADEQUATE PASSWORD CONTROLS, INADEQUATE PHYSICAL SECURITY, INADEQUATE SECURITY OR MANAGEMENT OF TAPE LIBRARIES, AND SAFETY OR FIRE HAZARDS.

- One Statewide system's data entry passwords represented the only access control, and anyone with entry and password knowledge could access all data from any of the system's 28 terminals. Food Stamp user IDs and

BEST COPY AVAILABLE

passwords were posted on a wall and some of the terminals; traffic throughout these areas regularly included employees with no authority to operate the system's files. In addition, employees had passwords that did not restrict them to only those programs they were responsible for, thus allowing them to access the food stamp and other data bases.

- At another Statewide system, the State Agency had issued 22 electronic access cards to computer center personnel, commercial vendors and construction workers, without a record of issuance. Physical security controls were also lacking over rooms containing ADP hardware and software.

INPUT/OUTPUT CONTROLS AND SYSTEM SOFTWARE CONTROLS

INPUT/OUTPUT CONTROLS AND SYSTEM SOFTWARE CONTROLS WERE INADEQUATE IN MOST INSTANCES. PROBLEMS FOUND INCLUDED: SYSTEM ACCESSES NOT LOGGED, TERMINALS NOT SHUT DOWN AFTER A SET NUMBER OF INVALID ATTEMPTS, NO PASSWORDS, OR PASSWORDS NOT SUPPRESSED ON REPORTS AND PRINTOUTS.

- Security software did not shut terminals down in one Statewide system after a repeated number of invalid access attempts.

- We found that one large multi-county system could be updated by 53 unsecured terminals which should not have had the capability to do so. We were unable to determine if any data had been entered from these terminals, because records of transactions were maintained for only 2 days. We further noted that passwords had not been changed in at least 10 years.

BEST COPY AVAILABLE

- At another Statewide system a software package to prevent access to system files did not protect files containing personal and medical data. About 300 SA users could read and modify the program files, although only a few of the users were responsible to maintain the files. Also, the system log which recorded all access attempts was not routinely reviewed for unauthorized access attempts.

CONTRACTOR SYSTEMS PROCESSING GRANTEE PAYMENTS

ONE OF THE 13 SYSTEMS INCLUDED IN OUR AUDIT WAS A CONTRACTOR-DEVELOPED SYSTEM. WE NOTED THAT THE CONTRACT FOR ADP SERVICES DID NOT INCLUDE SUFFICIENT SECURITY REQUIREMENTS TO ENSURE PROTECTION OF DATA AND PAYMENTS. For example, separation of incompatible functions was inadequate, and data input/output controls needed strengthening. ALSO, THE CONTRACT DID NOT SPECIFY THE AUTHORITIES OF THE DEPARTMENT AND GAO TO REVIEW SYSTEM OPERATIONS, PROGRAMMING AND RELATED ACTIVITIES.

FNS OVERSIGHT

FNS NEEDED TO IMPROVE ITS MONITORING AND OVERSIGHT OF ADP SECURITY. FROM FY 1983 THROUGH MID FY 1985, THE SIX FNS REGIONAL OFFICES (WHICH MONITORED 42 STATEWIDE WIC SYSTEMS, AND 38 STATEWIDE FOOD STAMP PROGRAM SYSTEMS; 5 STATES HAD MULTIPLE COUNTY-WIDE ADMINISTERED FOOD STAMP PROGRAM SYSTEMS) THAT WE AUDITED MADE ONLY TEN REVIEWS THAT INCLUDED ADP SECURITY MATTERS, RANGING FROM FOUR BY ONE OFFICE TO NONE BY TWO OTHERS. IN ADDITION, THE DOCUMENTATION WAS LACKING TO SUPPORT THESE REVIEWS IN MOST CASES, AND THE REVIEWS GENERALLY DID NOT DISCLOSE PROBLEMS SIMILAR TO THOSE FOUND BY OUR AUDIT.

BEST COPY AVAILABLE

Although a significant amount of guidance has been promulgated by OMB, the National Bureau of Standards, GAO, and the Department on the need to establish strong ADP controls over Federal systems, FNS HAS NOT DELINEATED MINIMUM SECURITY REQUIREMENTS FOR ITS GRANTEES. FNS'S POSITION IS THAT OMB CIRCULARS AND FEDERAL REGULATIONS DO NOT PROVIDE THAT FEDERAL ADP SECURITY REQUIREMENTS APPLY TO NON-FEDERAL SYSTEMS. FNS ALSO MAINTAINS, AND OIG AGREES, THAT THE ISSUE CROSS-CUTS FEDERAL AGENCIES AND PROGRAMS, AND THE OPTIMUM RESOLUTION WOULD BE A FEDERAL ADP SECURITY REGULATION WHICH WOULD APPLY TO ALL FEDERAL PROGRAMS. IT IS ALSO OIG'S OPINION THAT THE STATE AGENCIES ARE ULTIMATELY RESPONSIBLE FOR THE IMPLEMENTATION OF ADEQUATE ADP CONTROLS OVER THEIR SYSTEMS, HOWEVER IT IS INCUMBENT UPON FNS TO MONITOR THE ADEQUACY OF THIS IMPLEMENTATION.

FNS HAS AGREED TO INITIATE SEVERAL ACTIONS IN LINE WITH OUR RECOMMENDATIONS TO STRENGTHEN ADP SECURITY AT THE NON-FEDERAL LEVEL. FNS WILL EXPEDITE WRITTEN NOTIFICATION TO ALL THE STATE AGENCIES OF THE IMPORTANCE OF ADP SECURITY AND DEVELOP INITIAL GUIDELINES EXTRACTED FROM THE FEDERAL INFORMATION PROCESSING STANDARDS. (AS PREVIOUSLY NOTED, THE STATE AGENCIES REVIEWED BY OIG HAVE INITIATED ACTION TO CORRECT THE CONDITIONS CITED). FNS WILL WORK TOWARDS INCORPORATING THESE PROVISIONS INTO ITS REGULATIONS, STREAMLINE ITS MONITORING AND OVERSIGHT TO EMPHASIZE ADP SECURITY, AND REQUIRE ADEQUATE CONTROLS OVER NEW SYSTEMS AND MAJOR MODIFICATIONS TO EXISTING SYSTEMS WHERE FNS PARTICIPATES IN THE FUNDING. FINALLY, FNS WILL WORK WITH USDA CENTRAL GUIDANCE AGENCIES, THE DEPARTMENT OF HEALTH AND HUMAN SERVICES, AND OMB TO PROMULGATE RECOGNIZED ADP SECURITY STANDARDS TO ALL NON-FEDERAL ENTITIES WHICH PROCESS FEDERAL DATA.

MR. CHAIRMAN, THIS CONCLUDES MY REMARKS. THANK YOU.

BEST COPY AVAILABLE

Mr. GLICKMAN. Our last witness is Dr. Robert Conley, president, Conley Associates, formerly Deputy Assistant Secretary for Advanced Technology and Analysis, Department of the Treasury.

Mr. Conley, it's a pleasure to have you here. Your entire statement will appear in the record. You may summarize if you wish or read your statement.

Mr. CONLEY. I believe I will try to summarize.

Mr. GLICKMAN. OK.

STATEMENT OF ROBERT E. CONLEY, PRESIDENT, CONLEY & ASSOCIATES

Dr. CONLEY. I would like to state for the record that, while at the Treasury Department, and as chairman of the Subgroup on Telecommunications Security created by NSDD 145 that HHS was invited to attend the meetings. In fact, we invited all of the Government agencies. It was somewhat of a concern because, if all Government representation came, we could not find a room large enough.

In preparing my statement, I was somewhat concerned in how the subject should be approached, either from a technical, economic, legal, political, or even philosophical point of view. I chose, after consideration, to approach the subject as a system and to characterize the situation we find ourselves in, which is part organizational and part in the technological growth which we find in the areas of computers and communications.

So, in summary, I point out that the problem is that we have something which can be called an information system. It is a conglomerate of computers and a communications system. As such, it will cut across organizational lines, including different Government departments. In other words, there are systems which no single Government agency is in charge of because of the system interconnection.

Important to the process of understanding where we're going and how fast we're going, is to focus on the information system as a whole and not on its component parts being computers or communications.

Given this approach, then one of the primary things that the Government has to do, in my opinion, is to define the bounds of the systems. In many cases a transaction from one computer which is handling financial data, say, in the Treasury Department will transfer funds to a computer which is handling similar information in HHS, but it could also be handling a number of other things, including payroll or personnel information. Therefore, legislation impacting the Treasury Department may well mean that that transfer of funds is not protected until both departments have modified their computer complex.

The information system as a whole needs to be defined, then the vulnerabilities associated with it. In some cases the vulnerabilities will be different, depending on the type of system and the type of transfer. It is important that we define the system bounds. Then we can talk about the vulnerabilities and even develop capabilities to protect the system from unauthorized access.

BEST COPY AVAILABLE

The second area which requires a holistic approach is the policy direction as to what needs to be protected and what does not. We altogether get too enamored by the protection of computers and the technological aspects associated with it, and we forget that the information is really the thing that we're trying to protect.

In that regard, I proposed in the written testimony three basic categories. The first category is national security. This is fairly well defined, clearly defined, as a matter of fact as top secret, secret and confidential. There are some areas of unclassified but of national security nature; those I would relegate to the second category.

The second category is sensitive. And it's a category; it's not a classification.

And the third category is the public domain. That is, the Government is entrusted with information which is really in the public domain and therefore should be made available to the public. I would say in this case the Government has a responsibility to protect the information from manipulation and consequently still has an obligation for information security.

The category that is new is sensitive, and it has to be afforded some kind of protection. What that protection is needs to be spelled out. It is different than national security. And it needs to be developed. We are in the process of understanding or trying to develop the procedures and the techniques. When I say techniques, I am talking about techniques which are user friendly. People talk about passwords. The reason why they are pasted up on machines and everything else is that it is very difficult to change and operate daily if you're changing your call signs or your password. So, you're really talking about encumbering the individual when you place the security restriction on them. The rules must be written with care and understanding, not necessarily in a blanketed form.

These two areas are important: One, define what the system boundaries are; and two, define the categories of information requiring protection.

This concludes my remarks. If there are any questions.

Mr. GLICKMAN. Thank you. I appreciate, Dr. Conley, your remarks.

I would ask you, first of all, you have been involved in this issue for some time. Your resume is quite impressive. I have asked for your general comments concerning the GAO's overall assessment of computer security in Federal agencies as well as its comments on specific weaknesses.

Dr. CONLEY. Their findings did not come as a surprise to me. I would expect that the communications and computer systems have grown in an uncontrolled manner over the years. We are somewhat fortunate in the new systems which are being purchased. I believe we can incorporate proper techniques in the new systems. But it does not surprise me that the GAO found the current information systems lacking in security.

May I say one other thing regarding their survey?

Mr. GLICKMAN. Sure.

Dr. CONLEY. While in the Treasury Department, I found that there were almost too many people involved in this process. We had surveys to answer which were Treasury-wide, and that's a lot of people and a lot of systems, which asked for very similar infor-

BEST COPY AVAILABLE

mation, the questionnaires came for the GAO, OMB, OTA, and the GSA. All four were asking for very similar information, which caused the organization to do a considerable amount of work. I think it would be appropriate that the information being requested have some common baseline for comparison.

Mr. GLICKMAN. OK. Under the Paperwork Reduction Act, OMB is supposedly a focal point developing policies in this area. And you talk in your statement about the need to have, you know, a focal point in government. When you were at Treasury, what interactions did you have with OMB? Did OMB oversee implementation of its guidance?

Dr. CONLEY. Well, in the A-71 risk assessment which was put out, we did talk to the OMB personnel and exchanged information as to what we were doing and asked for guidelines. They did give us guidelines, but they had no real examples of what to be done, because they expected each agency or department to execute based upon the guidelines that they had given. In doing so, not wanting to reinvent the entire process again, we used a risk assessment that was developed by NASA. Intergovernment relationships, were aided by OMB, to exchange information. So, they helped.

We also wrote directives in order to implement the assessment and to give it further clarification.

Again, one of the problems with general guidance is you're operationally limited, and not always in charge of the entire system over which you must make the risk assessment. When a system is jointly owned, government agencies must cooperate since both require funds, and both go to OMB in a separate budgetary processes. So, it's difficult.

Mr. GLICKMAN. The final question I would ask you is, as one who was involved in the NSDD 145 process, how would you characterize the approach that would assign responsibility for unclassified systems to the National Bureau of Standards? If you've taken a look at H.R. 2889, this is what Mr. Brooks and his Committee on Government Operations has proposed.

Dr. CONLEY. Going back again, the techniques that are applied to protect unclassified information—I believe GAO and even the IGs mentioned this—are very similar in nature to that which you would have for national security. There aren't all that many new inventions involved in the process.

I think it would add further confusion to the process of who's in charge, whether it be the NSA, OMB, or the Department of Defense. But I have absolutely no hardship at all with the fact that education should be provided to the Government. But I think that the Government should clarify who's doing what to whom. It's difficult to go to OMB for one thing, GSA for another, the National Bureau of Standards for another, the National Security Agency for another, simply because I have two kinds of data in my computer. In some cases for the economy of scale you will want two types of data in your computer. You will want unclassified data and classified data on the same computer. The vagaries of not having that capability is at least two separate terminals on every ones desk: one for the unclassified machine, and one for the classified machine.

BEST COPY AVAILABLE

As a practical matter, it is difficult to separate the unclassified, if you will, from the classified and the techniques which are applied to both.

Mr. GLICKMAN. Well, there may actually not be any difference between the two. But at the same time, there's this kind of general reluctance on the part of the civilian sector to delegate the responsibility for an unclassified system to a military side of the government.

Dr. CONLEY. As a matter of fact, the costs associated with the military equipments involved are prohibitive for most civil agencies to purchase and place in their system. The impetus to produce lower cost crytographic techniques and procedures is under way by the National Security Agency.

I would say if you are going to establish another responsibility in this area, the National Bureau of Standards, that it would be appropriate that it be clearly linked to the NSDD 145 process today. The NSDD does take into consideration a system approach as opposed to a single computer or communications network, and also looks at the physical vulnerabilities associated with it.

I would say if training responsibility is properly linked and the Government doesn't confuse itself, it's a very positive approach.

Mr. GLICKMAN. Well, we know that never happens.

Dr. CONLEY. It never happens? Yes, sir.

Mr. GLICKMAN. Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman.

Doctor, on page 6 of your testimony, you state the Government should identify a focal point for this activity for both itself and industry, and I'm talking about how much security is needed.

In your opinion, where should the focal point be for computer security? Should it be OMB, GSA, NBS?

Dr. CONLEY. Well, for budgets to buy computers and new information systems, it ought to be an OMB responsibility to ensure that the Government is enforcing proper procedure on new systems and the funding is allocated to support it. I think when it comes to technical aspects, it ought to reside with that organization which has had it for the longest. That would be the National Security Agency and the Department of Defense. With a proper understanding and dialog between OMB and NSA, the process could be improved.

For the commercial world and interface standards associated with computers and communications, I believe NBS plays a major role and could be supported by the NSA.

Finally, I would say the necessary capabilities currently exist but are in different Government organizations. What is needed is a group to oversee and coordinate the activity. The group should be at a level within Government consistent with the task and critical nature of the problem.

Mr. LEWIS. You also stated that if the public communication network is used to connect terminals to a computer complex without encryption, unauthorized access must be assumed. Are you saying that any information that needs to be protected should be encrypted?

Dr. CONLEY. No. I am just saying that one ought to be aware of the fact that, if he is using public communication lines, he has no

BEST COPY AVAILABLE

control over how those communications are going to be directed. Therefore access can be obtained to the information. That's all I am saying. One just must be aware of that.

Let me give an example where the public network can be used without message encryption. In electronic funds transfer, the data or the actual message which transfers the money from my account to your account is not encrypted. The encryption process is a tag that is added to it to ensure that no one manipulates that message between the point of origin and where it's received. In this case, the information transferred can be read by anyone, What is necessary is that it has been authenticated and not altered in this process of transfer.

So, there's a case where the public network can be used without any problem.

Mr. LEWIS. Thank you.

Mr. GLICKMAN. Thank you.

Mr. Brown.

Mr. BROWN. I have no questions.

Mr. GLICKMAN. Thank you, Dr. Conley, for your excellent testimony today.

I thank all the witnesses.

We hold a hearing tomorrow on further subjects of this bill, including a more specific review of H.R. 2889 as amended by the Government Operations Committee.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned, subject to the call of the Chair.]

[The prepared statement of Dr. Conley follows:]

BEST COPY AVAILABLE

STATEMENT BY ROBERT E. CONLEY, PRESIDENT, CONLEY & ASSOCIATES, INC.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to testify on the subject of computer and communications security. The subject takes on many forms depending upon the background, understanding, and interests of the individuals involved. It is my intent to treat the subject as it applies to an information system with a viewpoint hopefully contributing to the committee's deliberations.

The situation which we face today is increased automation in nearly every aspect of our society. The introduction of computers and their networking in government and industry has brought us closer to the promised "Information Age". The promise being world access to information supporting an efficient and better understanding of day to day functions to be performed in a fluid and open society. With this promise comes a responsibility for controlling access to information which is the subject of concern.

Today's information systems (combination of computers and communication networks) have evolved from technological advances occurring at different times - namely the disciplines of communications and computers.

Communications and related security protection have matured since World War II. However, the economics of the market place over the last two decades have driven computer designs to architectures which have as their goal increased storage capacity and maximum openness and accessability. Security of selected

BEST COPY AVAILABLE

files was not a major market place concern. The power of a computer is to be a general purpose machine, applicable to many problem areas through software programming. This design thrust and general nature of software makes the computer and its operation today unpredictable. Software can be changed and go virtually undetected which limits the reliance to be placed on these systems without considerable oversight or knowledge.

The ability to limit access to data within an integrated computer complex is being developed and the research should be supported. Such protection will change current computer designs and require several years to mature. Another decade will be needed to reach operational application within government. Thus, todays information systems must be reviewed and care exercised to protect information while technology for computer security matures.

The information systems which have evolved have security as a system problem. The user or responsible parties operating the system desire assurance of the integrity of the information system as a whole. Since the security for the systems comes at a cost it is desired that the protection afforded is balanced. That is, dollars spent for communications security should not be excessive when compared to that associated with the computer complex or the procedures which screen individuals with access.

BEST COPY AVAILABLE

Security of information being a system problem requires some fundamental understanding. Specifically:

- The bounds of the information system must be known.
- The value of the information must be clarified.

Given that the bounds of the information system are known then access can be identified and measures of protection taken. If the public communications network is used to connect terminals to a computer complex, without encryption, unauthorized access must be assumed. Passwords which are used to gain access by public telephone lines are also points of vulnerability.

A technically difficult situation in computer networks is the task of protecting information which is limited to a subset of the authorized users. Multilevel security is the term associated with this situation and is the subject of current research.

The information to be protected is another area which requires clarification. Today there is no common accepted definition of what needs protection and what does not. Three

BEST COPY AVAILABLE

categories of information seem appropriate. These are:

- National Security
- Sensitive
- Public domain

As a matter of policy the categories are sufficient to determine if protection is required. The means by which protection is provided and, how much, remains debatable.

National security information is defined by a series of Department of Defense documents with a major organizational commitment and is the most stringent of security requirements. Information in the public domain requires the least amount of protection. Information available to the public which is provided by the government, however does not escape requirements for protection. If the government is making available information in electronic form it has a responsibility to assure that this information has not been changed or manipulated. Areas like weather, tax information, patents, etc. are all subject to this form of protection.

Sensitive is a category of information which is neither of National security nature or in the public domain. If the information is not in the public domain it should require a form of protection or an established audit trail for access.

BEST COPY AVAILABLE

Information would be categorized as sensitive if its manipulation or disclosure resulted in

- loss of life
- loss of property
- loss of privacy
- an unfair advantage in the market place, or
- violation of existing laws

NSDD - 145 made a positive step when it recognized security for information systems required a marriage between computer and communications security. This positive step should in time bring the separate technical disciplines of computers, communications and security toward a system application. Education and training of managers responsible for information systems, making them aware of the vulnerabilities and means of protection is also necessary. This will increase the general awareness and lead to corrective actions where glaring vulnerabilities may exist.

An example of the need for protection and common methods for its implementation is government electronic funds transfer. Manipulation of this type of information changes ownership of money or securities. The value of the information is easily established.

Initiatives in government for improved cash management focused attention on the process for money transfer. With the prime interest rate at 18% in the early 80's a one day delay in

BEST COPY AVAILABLE

handling the transaction or "float" on a billion dollars equated to 49 million dollars in interest. The float in some cases being in excess of 5 days gave an impetus to electronic funds transfer systems.

Recognition of the vulnerability if these transfers were not properly protected or tagged providing an audit trail resulted in the Secretary of Treasury issuing a directive on 8/16/84 to protect all Department of Treasury electronic funds transfer by 1988 through authentication. In addition the directive established the method of authentication available to the banking industry as a means to accomplish the objective.

Following the directive on electronic funds transfer protection it was recognized that similar protection of electronic files for enforcement was appropriate. A Treasury directive was issued on 2 April 85 "Information Systems Security" which was applicable to all information systems within the Treasury Department.

How much security is needed? This is a question which deserves an answer or proper guidelines for its implementation. The government should identify a focal point for this activity for both itself and industry. If electronic security could be purchased by the yard a risk assessment of information loss could be traded off for a specified amount of protection. Unfortunately security is a complex and dynamic process which requires continued attention. The security techniques of the past have always needed to be upgraded as the

BEST COPY AVAILABLE

capability of the threat grows and the reward for exploitation increases.

In conclusion the government should maintain an understanding of the information systems it operates, define the information to be protected and develop proper procedures against loss or unauthorized access. In addition, the government should establish standards which provide guidelines for commercial application in concert with industry.

Mr. Chairman, this concludes my prepared testimony. I will be pleased to answer any questions that you or the Subcommittee may have.

BEST COPY AVAILABLE

Biographical Sketch
of
ROBERT E. CONLEY

Dr. R.E. Conley born in Akron, Ohio on 12 Oct. 39 received a B.S. Degree in Electrical Engineering from the University of Akron, Akron, Ohio, a M.A. Degree in Applied Mathematics from the University of Maryland, College Park, Maryland and a Doctorate degree in Computer Science from the George Washington University, Washington D.C..

Presently he is president of Conley & Associates Inc., a consultant service in command, control and communications intelligence and information systems.

He held the position of the Deputy Assistant Secretary for Advanced Technology and Analysis with the Department of the Treasury from 1983 to 1985. His previous position was Navy Chief Scientist for Command and Control Programs (1974-1983). Dr. Conley was selected for that position in the Navy following 18 years in various assignments with the National Security Agency including three years of active duty as an officer with the USAF.

BEST COPY AVAILABLE

FEDERAL GOVERNMENT COMPUTER SECURITY

WEDNESDAY, OCTOBER 30, 1985

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE AND TECHNOLOGY, SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS AND SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY,

Washington, DC.

The subcommittees met, pursuant to notice, at 9:36 a.m. in room 2203 Rayburn House Office Building, Hon. George E. Brown, Jr. (chairman of the Subcommittee on Transportation, Aviation and Materials) presiding.

Mr. BROWN. The subcommittee will come to order. Today we are joining with our colleagues from the Science, Research and Technology Subcommittee to hear testimony on H.R. 2889, the Computer Security Research and Training Act of 1985.

The need for H.R. 2889 was identified in hearings held just about 1 year ago before this subcommittee. At that time, we noted that the Federal Government had become totally dependent on automated information systems to perform a multitude of essential services. Furthermore, the information stored in Government computers and transmitted over various communications networks is vulnerable to unauthorized access and disclosure, to fraudulent manipulation and to disruption. The situation was described as the electronic equivalent of leaving the bank door unlocked.

We used to have a saying about barn doors, but I guess bank doors are more important today.

Yet, despite the potential serious consequences of these threats we found little evidence of an overall systematic approach to correcting this lack of security. Of particular concern was the level of security among people who operate, use and manage computers. Such people are extremely important in the security sense because, as studies have shown, they are the greatest problem. It is not the much publicized hacker working to penetrate from the outside; rather, it's the insider, one who already has authorized access, that causes the greatest damage in practice.

Yet, as we learned yesterday at our hearing from GAO's survey of 25 Federal computer systems, there is very little formalized effort made to reach these individuals to make them aware of system vulnerabilities and the importance of enhancing security.

The purpose of this bill, H.R. 2889, is to strengthen this weak link. It does this by establishing a research program at the National Bureau of Standards aimed at developing guidance for use by agencies in structuring computer security awareness training pro-

BEST COPY AVAILABLE

grams for their employees. It also makes it mandatory that such training be given periodically in each agency.

Since its introduction in June, H.R. 2889 has been moving rapidly through the legislative process. Yesterday it was ordered reported with amendment by the House Government Operations Committee, to whom it was referred jointly. Mr. Brooks' amendment in that markup in Government Operations keeps the original provisions of H.R. 2889 but expands the bill considerably in order to correct some of the defects in National Security Directive D-145 that were brought out in our hearings on this subject last summer. He does this by giving NBS broad authority to set computer security standards that would apply to all Federal computer systems currently subject to the Brooks Act—essentially all unclassified systems.

Our witnesses today have been asked to comment on H.R. 2889 as introduced. Since these instructions were given out, however, the Brooks amendment was passed by his committee; therefore, we will also want to hear any comments the witnesses may have on that amendment during the question and answer period.

And I might say it is at least some of our hopes on this committee that we can mark up this bill and jointly report it to the floor with the Government Operations Committee, so that we may hopefully get some action on this subject.

Do you have any comments, Mr. Lewis?

Mr. LEWIS. Thank you, Mr. Chairman. Few people would disagree that there are some serious problems with the security of the Federal Government computer systems. Yesterday we heard testimony regarding the results of a study of computer-related fraud and abuse among Federal agencies; 46 out of a total of 98 fraud cases were studied, and in every case studied, the perpetrator was an authorized user of the system. It is clear that a major part of the problems dealing with computer security are internal. Part of this can be explained by the lack of adequate training provided in this area.

In other testimony yesterday we heard GAO reveal that only 2 of 25 Federal systems surveyed met their criteria for training. Better computer security training programs won't solve all the problems, but surely it will go a long way toward providing more secure systems within the Federal Government.

The bill that we will be discussing today, H.R. 2889, seeks to remedy this situation by requiring the Federal agencies to conduct training classes in computer security awareness.

I support that purpose. As you know, I am a cosponsor of this bill. I am concerned, however, with the direction this bill has taken since introduced. I am referring to the amended bill as reported out of Government Operations Committee. This substitute bill seeks to dismantle NSDD-145 and much of the work already underway in this area.

Mr. Chairman, we have heard considerable testimony on NSDD-145 and even the critics of this directive acknowledge that it effectively addresses many of the recommendations made by this subcommittee.

Without going into all the perceived problems with this directive, I would merely like to point out that we should be very cautious

BEST COPY AVAILABLE

about using this bill to mandate major changes in this directive. I would further point out that the directive has only been in existence for a year, and although we have heard many fears expressed over what could happen, as yet I know of no instance where the fears have been realized.

Mr. Chairman, we all recognize the need for some sort of training program in this area, and I am hopeful that today's hearing will bring us a little closer to finding an appropriate solution. Thank you, Mr. Chairman.

Mr. BROWN. Thank you very much.

Mr. Packard, do you have any comments to make?

Mr. PACKARD. I have no opening statement, Mr. Chairman.

Mr. BROWN. All right. At this time I would like to call our first witness, Mr. James H. Burrows, Director of the Institute for Computer Sciences and Technology at the National Bureau of Standards, and we are pleased to have you here, Mr. Burrows. How is everything going down there?

Mr. BURROWS. As best it can be.

Mr. BROWN. You may present your testimony in any way that you see fit. The full text, of course, will appear in the record.

TESTIMONY OF JAMES H. BURROWS, DIRECTOR, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY

Mr. BURROWS. Yes, sir. It's a short testimony and I'd like to read most of it.

Mr. Chairman and members of the committees, thank you for inviting me to speak to you today about the Federal Government's needs for computer security research and training. This is an issue of national interest and concern, and we appreciate the attention that your committees and the Government Operations Committee are giving to this topic. These hearings will help to bring to the forefront the problems that accompany our increased use and dependency on computers, the solutions that are available and the roles and responsibilities of the various Government organizations with regard to computer security.

As you know, the Institute for Computer Sciences and Technology at the National Bureau of Standards carries out a program of research in computer security as part of our overall responsibilities under Public Law 89-306, the Brooks Act.

In addition, responsibility for developing computer security standards and guidelines is specifically assigned to the Department of Commerce under the Office of Management and Budget circulars and has been delegated to NBS. The Paperwork Reduction Act also provides additional legislative authority to carry out our program.

As you mentioned, while hacker incidents and fraud and computer-related crime from the outside have received attention in the press, they are not the only cause for concern. Serious losses also result from processing incorrect data and interruptions to data processing, and internal defalcation.

Federal programs and services that affect the public must be carried out accurately and in a timely manner to maintain citizen confidence and trust in the Government. ISCT's activities in computer

BEST COPY AVAILABLE

security are part of its technical program to assist Federal Government organizations.

Security is a part of, the integral part of, overall systems planning; therefore, we must address computer security in all aspects of computer system development and operations, not just on the side. This includes software systems, networks, storage media, hardware components, interfaces, everywhere. The weak link can appear anywhere in a complex system, and a comprehensive approach is needed to assure that strengths in one part of the system are not wiped out by weaknesses elsewhere.

We leverage our efforts by working closely with computer users in other government and private sector organizations, the computer industry, voluntary standards organizations and research groups. As a result, we are in a position to look at the broad range of problems and develop a broad range of solutions that are cost effective and widely applicable. We can pull together different efforts and achieve change by working with others.

Our research efforts are directed toward solving problems common in the Federal agencies. We work closely with the agencies doing computer security research in order to avoid duplicating their efforts and to be able to transfer our work and their work to the other organizations.

In particular, we are working on computer security with the National Computer Security Center, which is investigating the development of secure technology for national defense and national security-related applications. I understand Dr. Brotzman is testifying today on the activities of that Center.

Other organizations such as DOE, DARPA and the Defense Communications Agency are involved in research in computer security that addresses their unique requirements to protect special purpose critical systems.

There are many areas where research would have broad application both in Government and the private sector, and they require greater attention. For example, research in the areas which are—that could make a difference in our ability to protect computer information and systems that will be used in the next 5 or 10 years are an integrated technology security in networks; networks linking different computer technologies such as large computers, minicomputers, microcomputers, et cetera, are the goal of the international standards efforts and will result in improved data sharing and distributed processing capabilities.

At the same time, however, the vulnerability of data to unauthorized modification and disclosure will be increased. We must develop architectures, protocols, and techniques that will allow secure data processing and data communication between these different systems in a network.

In the area of personal identification and authentication, networks will not be secure unless we have cost effective methods for authenticating the identity of computer users. It looks like the small cards the size of a credit card which are called Smart cards, which are coming into play in the banking area in the near future, give us an opportunity to get new means of personal identification authentication.

BEST COPY AVAILABLE

But we need means of coupling the information on that card with the computer transactions performed by the user to assure that only the proper person is carrying out the authorized transactions.

Other personal identification and authentication methods need to be improved—use of fingerprints, voice prints, signatures and passwords could be used to prevent, also, unauthorized access to systems, although they may not be as—as costly, but not as effective.

In security variance detection, we keep a lot of records on what's going on inside the computer but we need automated tools that will capture the computer security-related events and provide automatic processing of the audit trails in order to highlight suspected computer security problems. We particularly need audit trails that are suitable for use by nontechnical management personnel

So to address today's problems, we must take three steps. We must first stimulate management and user awareness of the need for computer security. Second, we must provide information about the safeguards that are currently available, and we must conduct research and develop techniques and methods that keep up with the changing technology. This is vital in a campaign to improve computer security.

I believe that the legislation addresses clearly-established needs for computer security research and for training the people who manage, use and operate Federal Government computers.

It's also clear that the research and awareness programs must be directed toward better methods of reducing vulnerability to accidental events, as well as computer-related crime and fraud. Such safeguards against accidental events have a twofold effect; they reduce the potential for harmful effects and they reduce opportunities for fraud and abuse. Users can take advantage of these errors and flaws in systems to commit computer-related crimes.

As we know, more losses occur from accidents, errors and omissions than from any other types of activities. Numerous methods are already under development in our current programs and we expect to get into more areas in the future.

However, we believe that the Brooks Act already provides NBS with sufficient authority to develop the methods to address the security problem. Our current role in computer networking involves research and standards developed for the communication of digital data between computers and computers, and computers and terminals.

H.R. 2889, the substitute bill reported by the Subcommittee on Legislation and National Security on October 23 and by the full Government Operations Committee on October 29, extends to NBS the sole authority and responsibility for management, research, and training of personnel to assure the security of computer and telecommunications systems subject to the Brooks Act.

Deputy Secretary Brown has expressed our opposition to the substitute bill in a letter to Chairman Brooks dated October 29, and there is a copy of that letter attached to my testimony.

We appreciate the committee's concerns with our national computer security problems, and I am ready to answer any questions that you have.

BEST COPY AVAILABLE

Mr. BROWN. Thank you very much, Mr. Burrows.

Do you have any questions, Mr. Lewis?

Mr. LEWIS. Yes, sir. How would H.R. 2889 affect NBS, Mr. Burrows?

Mr. BURROWS. H.R. 2889, as originally drafted, would give us a nudge to probably spend a larger percentage of our budget on computer security. We currently spend about 10 percent of our budget on computer security. We would probably get a lot of cooperation from OPM and others in terms of getting on with getting a national training program going.

Mr. LEWIS. Has NSDD-145 had any adverse effect on NBS's activities in computer security?

Mr. BURROWS. To date, I can see no adverse effect. It is slightly confusing in who has control. It is, I think, to our advantage to have a diffusion of new money and new people into the activity. The activity never has had very many players, and I think new players are needed to get on with the job.

Mr. LEWIS. Did I understand you to say in your testimony—and I will turn the page over—that the Brooks amendment covers the security that you need?

Mr. BURROWS. The Brooks amendment is contrary to what the Department believes should be done.

Mr. LEWIS. I see. I meant the Brooks Act. I didn't mean the Brooks amendment; I meant the Brooks Act.

Mr. BURROWS. Well, the Brooks Act has adequate authorization to work on the computer security problem and to produce anything we can afford to produce.

Mr. LEWIS. What in your opinion do you feel 2889 will do for you that what we already have will not do?

Mr. BURROWS. In terms of alerting people to the requirement to do training and getting OPM at least alerted to the fact that the Congress wishes that they make sure that there is a training program, I believe that that is new. I don't believe there is any OMB directive or any other directive currently which tells people that they must do things and also asks them to report on how well they are doing.

Mr. LEWIS. I guess one final question. Is there any evidence that the representation on the NTISSC has any negative effect on the civilian agencies and their concerns?

Mr. BURROWS. I really can't talk for the civilian agencies. As a whole, I have heard comments to the point of "Thank God we're finally doing something," and why did it have to be DOD? But everybody is pleased that something is being done, I believe.

Mr. LEWIS. Thank you, Mr. Chairman. Thank you, Mr. Burrows.

Mr. BROWN. Mr. Packard?

Mr. PACKARD. Thank you, Mr. Chairman.

Do you have any estimate or have any studies been done to determine the cost to the Bureau of Standards of computer abuse?

Mr. BURROWS. The cost to the Bureau of Standards of computer abuse or the cost to the Government of computer abuse?

Mr. PACKARD. I would like to know your own Department first.

Mr. BURROWS. I don't know any study that has been done. We have issued directives on how to avoid having security problems, how to protect the computer installation and its information. Most

BEST COPY AVAILABLE

of the information is not of a sensitive or classified nature, and it is pretty much open to anybody to get access to, through the Freedom of Information Act.

Mr. PACKARD. Do you have estimates as to what the total figures might be in terms of Government losses?

Mr. BURROWS. I think the IG operation, and they are working in the area of fraud and abuse, has pulled together almost the only information we have on the Government's activity, and I think that was reported on yesterday by Kusserow. That group is the group that has the authority to collect the information. I don't have any authority to go out and collect information of that variety.

Mr. PACKARD. Do you think we are making the kind of progress that is needed to curtail the fraud and abuse that is existing now in Government organizations and agencies? Are we doing all that can be done?

Mr. BURROWS. No, sir. I think it is amazing. I think it is more a lack of attitude, and having the right attitude and realizing that you have information which is a public trust kind of operation and realize that you should protect it and make it available and at appropriate times but protect it at other times. Until that becomes a part of your job statement and you get told when you don't do it that something will happen, and it is made clear that it is really a part of keeping the activity moving appropriately, until that is done, an awareness of the requirement for security, I think we will be wide open for a long time, to almost anybody.

Mr. PACKARD. Is the Brooks Act adequate to address those shortcomings that you have just mentioned?

Mr. BURROWS. I think just management common sense is the only thing that will do that.

Mr. PACKARD. That is going to require some educational——

Mr. BURROWS. That's correct.

Mr. PACKARD. Do you see that kind of activity taking place or planned?

Mr. BURROWS. I believe that Dr. Brotzman will talk about their activities, which is probably the largest education program that I see going at the moment.

Mr. PACKARD. In other words, you sense that there is a serious problem that is not being adequately addressed at the present time?

Mr. BURROWS. That's correct. When I go out and visit bankers and insurance companies, I get one feeling. When I visit Government installations, other than DOD, I get a feeling that it is not only on the surface but deeply embedded in the organization. When I visit DOD and some installations, I get it on the surface, but it is missing underneath.

Mr. PACKARD. Are you suggesting that we can learn something from the private sector in terms of better computer security?

Mr. BURROWS. I think we can learn possibly how to motivate people.

Mr. PACKARD. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Boehlert?

BEST COPY AVAILABLE

Mr. BOEHLERT. Mr. Chairman, I have an opening statement. I ask unanimous consent that it appear in the record following your statement.

Mr. BROWN. You may read it if you wish.

Mr. BOEHLERT. I don't think that is necessary.

Mr. BROWN. Without objection, it will appear.

[The prepared opening statement of Mr. Boehlert follows:]

BEST COPY AVAILABLE

OPENING STATEMENT
HONORABLE SHERWOOD BOEHLERT (R-NY)
RANKING REPUBLICAN MEMBER
SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY
OCTOBER 30, 1985
H.R. 2889, COMPUTER RESEARCH AND TRAINING ACT

WE HAVE KNOWN FOR SOME TIME OF THE PROBLEMS ASSOCIATED WITH OUR INCREASING DEPENDENCE ON COMPUTER TECHNOLOGY AND ADVANCED COMMUNICATIONS SYSTEMS. OUR ADVANCE IN TECHNOLOGY IS PERMITTING A PHENOMENAL CAPACITY TO PROCESS DATA, BUT AT THE SAME TIME OUR DATA IS INCREASINGLY VULNERABLE TO COMPROMISE THROUGH ELECTROMAGNETIC EMANATION AND UNAUTHORIZED ACCESS. THIS AFFECTS OUR LIVES IN NUMEROUS AREAS RANGING FROM NATIONAL SECURITY ISSUES TO THEFT OF OUR FRONTIER TECHNOLOGICAL DATA BASES TO OUR OWN PERSONAL ACCOUNTS. SEVERAL HEARINGS HAVE OCCURRED WITHIN THE LAST YEAR TO HIGHLIGHT THESE ISSUES. IN 1965 WE CREATED WHAT IS NOW CALLED THE INSTITUTE FOR COMPUTER SCIENCE AND TECHNOLOGY (ICST) AT THE NATIONAL BUREAU OF STANDARDS. IN 1980 WE PASSED THE PAPERWORK REDUCTION ACT (P.L. 96-511). IN 1982 WE PASSED THE WARNER AMENDMENT TO P.L. 96-511. LAST YEAR THE ADMINISTRATION ISSUED NATIONAL SECURITY DECISION DIRECTIVE (NSDD)-145. ALL OF THESE HAVE ATTACKED THE GENERAL PROBLEM FROM DIFFERENT ANGLES, THEREBY ADDRESSING THEMSELVES TO DIFFERENT ASPECTS OF THE ISSUE. THEY APPEAR TO BE FUNCTIONING IN A COORDINATED WAY TO REACH A SOLUTION AND AREAS OF EXPERTISE HAVE DEVELOPED WITHIN THE DIFFERENT AGENCIES. WE MUST BE VERY CAREFUL, IN OUR ATTEMPT TO CREATE A BLANKET SOLUTION TO THIS UNIVERSAL PROBLEM, TO INCLUDE ALL ASPECTS OF INFORMATION SYSTEM SECURITY AND ALL OF THE AFFECTED USERS: GOVERNMENT AND PRIVATE. ONLY IN THIS WAY CAN WE EDUCATE OURSELVES AND INSURE THAT WE DO NOT FURTHER CONFUSE A VERY COMPLICATED ISSUE. I LOOK FORWARD TO THIS CHANCE TO HELP CLARIFY SOME OF THESE ISSUES AND WELCOME OUR GUESTS.

BEST COPY AVAILABLE

Mr. BOEHLERT. Mr. Burrows, I like what you say. It is refreshing for me to sit up here and hear people talk in terms of management common sense and lack of proper attitude. You are hitting the nail right on the head.

I think on page 5 of your testimony, you are talking about addressing today's problems. The key step is to stimulate management and user awareness of the need for computer security. That's a key step.

The witnesses we heard yesterday, GAO—and they were excellent witnesses—underscored that about 58 times.

What you are saying to me, if I interpret your remarks correctly, is we have what we need to do the job, only we are just not doing it, we are not properly motivated. We are not using good old fashioned common sense.

Let me ask you a specific question. Do you believe H.R. 2889 is an effective response to the perceived problems with NSDD–145?

Mr. BURROWS. It's a start. It takes money and it takes time.

Mr. BOEHLERT. And it takes commitment.

Mr. BURROWS. Yes.

Mr. BOEHLERT. Money, time, and commitment. If you had to prioritize them, would you not put commitment first?

Mr. BURROWS. You bet.

Mr. BOEHLERT. That's what I think is lacking.

Mr. BURROWS. That is right. I think commitment and an understanding, I guess, that loose operation is not just detrimental in terms of security. It is detrimental in terms of getting the job done.

Mr. BOEHLERT. Don't we have a problem with Government agencies? I have been exposed on a very limited basis to this, where you have supervisory people in positions of major responsibility who really don't understand the whole system and what is going on. Therefore, there is a lack of awareness of what is needed in order to provide the security that we desire.

Isn't that happening more and more in agencies of the Federal Government?

Mr. BURROWS. I think it is happening everywhere.

Mr. BOEHLERT. More so in the Government. The reason I say so is because of the unusual aspects of the civil service system.

Mr. BURROWS. I am a computer-nik. I believe, back in the 1950's and 1960's, we put some people out of business who we sorely need back, and that is the people who have the overall systems and procedures aspect and can tell management what the system does without talking about bits, bytes and all the technology, so that they can understand and see where the weaknesses are and where they can be had.

That is not a technology problem. That is an understanding your system problem. The systems have gotten so complex that very few people understand what they have working for them. Until they understand what they have working for them, they won't understand the weaknesses. Until they see they have weaknesses, they probably won't get committed.

Mr. BOEHLERT. That is the key thing, commitment. Thank you very much. No more questions, Mr. Chairman.

Mr. BROWN. Mr. Walgren, do you wish to put an opening statement in the record at this point and ask any questions?

BEST COPY AVAILABLE

Mr. WALGREN. Not at this point. It is hard to keep up with my ranking minority member, but we try. I will pass on the opening statement.

You mentioned, Mr. Burrows, that we dropped some systems people from the 1950's?

Mr. BURROWS. Back in the old days, sir, we used to know people in systems and procedures, who walked the paperwork and showed you how a document [1] was seen by two people, and important documents that committed money didn't get handled.

We had ways where we could see the system. It was open and therefore you could see how you could protect it. We now have systems which are buried. They are unavailable for examination. Most people don't even understand what they look like.

I think in that process, you somehow think it is in the machine and safe—and safe, it is not.

Mr. WALGREN. Sir, that's a level of understanding of the system that is lacking today, that the previous methods were perhaps more subject to?

Mr. BURROWS. Yes. I think we had simplier systems and they were more open to people to understand. Today we have very complex systems and they are not understood, even by the people who are building them.

Mr. WALGREN. Obviously somebody understands them. The private sector understands them. The banks understand them. The DOD understands them.

Mr. BURROWS. In many cases, that is true. In some cases, that is not.

Mr. PACKARD. Would the gentleman yield for a moment on that point?

Mr. WALGREN. I would be happy to yield.

Mr. PACKARD. Are you suggesting that because—the reason we are not doing more than we are doing, in terms of computer security, is because those who operate and manage the computers don't understand the kind of equipment and the capacity of the equipment they have?

Mr. BURROWS. No, sir.

Mr. PACKARD. Would that suggest then that they also are not utilizing that equipment to its fullest in terms of utility, not just computer security, but a failing to use it in areas that would be helpful, useful and productive in the simple operation of the equipment?

I have to assume that it is a two-way sword, and if they don't understand the equipment they have, sufficient to provide better security, then they do not understand it sufficiently to get the full utility out of it, which would be a significant loss.

Mr. BURROWS. I don't think there is as much a lack of technical expertise in the Government as people would like to point out. I just think that there is everywhere a cost of building a complicated system, documenting it, explaining it to the management, which sometimes is short circuited, both in civil practice and in the Gov-

[1] Important money-commitment documents were cosigned by separate and separated pensions in separate management chains.

BEST COPY AVAILABLE

ernment, and without understanding what you have there, you don't understand the importance of security.

I think banks who can see that money can dribble out here and there and know that is what they have to take care of and it replaces hard cash with computer records, it is very clear to them that they have to protect those.

Mr. PACKARD. I want to thank the gentleman for yielding.

I see a counterpart here though that is not the thrust of this hearing, but obviously, as something that would be perhaps more costly if we are not getting the full utility out of the equipment, the expensive and complicated equipment, and simply looking at the loss in terms of computer security may be shortsighted.

Mr. WALGREN. I don't know if this should come in terms of a statement, and the witness may or may not be able to comment on this, but it has been my impression, and I think others have the same impression, that we have under invested in new technology in the Government.

We were essentially freezing and capping and cutting ever since the inflationary cycle set in, in the late 1960's. You can see that when you graph some of the budgets.

One of the reactions to the escalating burden of Government was to under invest in both computers to begin with and apparently in the expertise to run them, and to run them most effectively.

I wanted to ask, can you give us some idea of the size of ICST and the size of the computer security program that you now have, and somehow measuring that off against the size of this pill or problem that we are attempting to solve? I would like to compare it to the idea that you can always find an agency in the Government or an effort in the Government to solve a problem, but if the effort is totally de minimis compared to the problem, you might feel good but you don't make an awful lot of progress on solving the problem.

How big at present is the ICST effort in computer security? Could you say that is less than 1 percent of what you would envision would be required if you were to take on the responsibility to actually do what the Brooks amendment would have you doing?

Mr. BURROWS. Our current work in the security area is funded through two means, through direct appropriations from Congress and through moneys given to us from other agencies, to help them on specific security problems.

The total amount of money which I spend in ICST is on the order of $13 to $14 million. It is probably less than 10 percent of that which is on security.

Mr. WALGREN. We are talking about $1.3 million on security?

Mr. BURROWS. Probably less than that. Probably closer to $1 million.

Mr. WALGREN. Now, what level of resources would be required to really say to one another honestly that we are making a successful effort to train all of the Government personnel that are involved with computers and to create the kinds of discipline that would be required to assure us that reasonable security is there?

Mr. BURROWS. I don't really have a feel for that. I think you can get some feeling maybe from Dr. Brotzman on the size of the effort

BEST COPY AVAILABLE

which they initially contemplated for getting on with this kind of activity in the Department of Defense alone.

I would also like to make a point that the money that gets spent in computer security or in making a system more effective, including the security aspect, is it is mostly spent not by the research and training groups, in terms of the trainers, but it is spent by the people who need the training.

I have talked informally with the Department of Energy, for example. Their budget, as they see it, for computer security, information security and their activity, is someplace between $10 and $20 million. They have a very good program.

Mr. WALGREN. In the Department of Energy?

Mr. BURROWS. That is correct. It doesn't do all the things they would like it to do.

Mr. WALGREN. I hope we can pursue at least a thumb nail measure or size that we are involved in here. If we graft this responsibility onto ICST, we either create what would be a very large entity within the NBS or we get ourselves into the one man in Tokyo syndrome, where we feel that we are getting access. We have a Government program to give us access to Japanese technical literature and when we look at what the program is, we have one man in Tokyo. It doesn't cover the problem.

Thank you, Mr. Chairman.

Mr. BROWN. Thank you very much.

I kind of wonder how you must feel, Mr. Burrows, when you see a group of Congressmen such as ourselves, and inferentially, Mr. Brooks and others, trying to provide a substantial additional increment to your responsibilities over there, without any additional money, at least in this bill, and another part of the Government trying to cut your budget in half.

How do you react to that? [Laughter.]

Mr. PACKARD. Is this on the record or off the record, Mr. Chairman?

Mr. BROWN. How do you handle schizophrenia?

Mr. BURROWS. I find planning very difficult to do.

Mr. BROWN. I would suspect so.

This emphasis that you have repeatedly made and which has been concurred in by members of the committee, on the importance of a committed and dedicated management with an understanding of systems, this makes me think back a generation to the development of quality control procedures in this country, which did not take off very well, but Professor Demming went to Japan and it took off very well over there.

They developed a committed management who understood the importance of integrated systems for quality control and made them the best manufacturers in the world.

Professor Demming has come back over here, or used to, go around lecturing management and telling them that all of their trade problems are their own damn fault because they are poor managers.

Essentially we are seeing the same thing here with regard to utilization of computers.

Is that analogy far fetched, or is it somewhere close to the mark?

BEST COPY AVAILABLE

Mr. BURROWS. I'm quite familiar with Dr. Demming's work and the work that we did during World War II. We really did bring our manufacturing capabilities up to quite high capability and dropped it after the war. I don't think that has happened in computers yet. It is still a developing area. We don't know all the answers.

I don't think it is the idea that we know how to do it exceilently but we know how to do it a hell of a lot better than we are doing it now.

Mr. BROWN. You did indicate that we had lost at least some of our capabilities in the way of systems' analyses.

Mr. BURROWS. There were some people put out of business by the computer people and we haven't gotten that general person with the overview to explain things to management back. [Laughter.]

Mr. BROWN. Insofar as lack of management understanding and dedication to resolving the problem of how we effectively use computers and telecommunications systems, how we provide them with security and protect privacy and do all these other things, then if we have a management that is defective in that regard it's the same kind of a system fault with the national as we had with the quality control after World War II. It could be just as hazardous to our economic health, it seems to me.

Mr. BURROWS. Oh, yes. Yes. I think the way we build systems is a crime in some cases.

Mr. BROWN. Getting to the specifics of your work, a good part of your funding, as you indicated, for the work you do in the Institute is external money. Does any of that come from the National Security Agency or Department of Defense?

Mr. BURROWS. I have gotten money from the National Security Agency, yes.

Mr. BROWN. It isn't a large part of the external fund?

Mr. BURROWS. I don't have a large part of money from anybody, but it could be several hundred thousand dollars, and it my grow or shrink depending on both their budgets and our ability to have people available.

Mr. BROWN. Do you have any problems in terms of coordinating the work that you are doing, which presumably is directed at civilian applications of computers in the Government with the work that's being done at NSA which is more directed at the classified and security needs——

Mr. BURROWS. I have no problems with that. I have been given access recently—although I have not yet gotten to go to one of their meetings, but I have been made a member of one of their planning groups and will understand where they're going besides just what they're doing right now. So I think we will have a more coordinated program in the future.

Mr. BROWN. Insofar as we're talking here about computer systems; that is, networks, which involve both computers and telecommunications systems, all of the related kinds of activities—that all falls within the scope of your responsibility, does it not?

Mr. BURROWS. In the telecommunications area, which has been an anomaly—the interface between telecommunications and computers has been a point of concern for sometime. I would say since the early fifties. And telephony is not really much of interest to the digital data people anymore, although there was a time when you

BEST COPY AVAILABLE

had to find a way to adopt telephone circuits for use in sending digital data over.

I am not really that interested in getting into the business of understanding media problems and how you go coaxial cable and that kind of thing. There's a lot of people in that business and we just are not in that.

But we are in the business of how you can tie—through those facilities, how you can tie computers together and computers and terminals together so you can send digital data around. And that turns out to be a problem that both of us have to attack; the telecommunicator has an act in that. If he doesn't give me the right service, I can't do the job. If we don't have an integrated system, I can't do the job, and so we have to work together.

But we have never really been in the telecommunications business per se; only the aspects of it which have to do with tying computers to computers and computers to terminals.

Mr. BROWN. But you would be concerned about the capability of the communications system to carry the computer data load, the traffic, I would presume, and the effect that that would have on——

Mr. BURROWS. Yes. But that area of the business I don't say is trivial—it's not—and there are a lot of digital switches in that kind of network, and we are interested in those switches. But when it gets around to ordering up capacity, people know how to deliver capacity and they know how to make capacity available. And so only in terms of how the network is designed and knowing that we have the adequate capacity. Other than that, from the systems point of view, telecommunications is a technician's game.

Mr. BROWN. Well, it's all a mystery to many of us on the committee. Our perception is that with the proliferation of large-scale data bases and high speed computers, that there is a rapid movement toward digitalization of the system with very broad band communication links such as optical cables and, in the not too far distant future, that that's going to be the model for operations.

Is that future going to be on us shortly, or is a long way off?

Mr. BURROWS. I think in different countries it will come at different times. In America it will come when it pays for itself. In some countries it will come earlier because they pay for it. But the thing called ISDN or IDN or whatever, the integrated digital network, is coming. It's cheaper, it's just a better deal all the way around.

Mr. BROWN. And you are trying to keep abreast of the standardization problems in that area, along with——

Mr. BURROWS. Yes. Most of that standardization work takes place in CCITT.

Mr. BROWN. Spell that out for me.

Mr. BURROWS. It's the Consultative Committee on International Telecommunications and Telephony.[1] That's an international—it's a part of a treaty organization. Let's see, what is it. It's the Union of International [2]—ITU, I guess.

Mr. BROWN. Yes, telecommunications union. But is NBS the responsible body for that?

---

[1] Consultative Committee on International Telegraph and Telephone.
[2] International Telecommunications Union.

BEST COPY AVAILABLE

Mr. BURROWS. No, we are not. The organization which represents the Government in that is the State Department. I have members of the some of the internal—within the Government and with industry committees. There is a subcommittee D which meets and talks about what's happening in that area. In addition, the American people who are in that business are members of the ITU.

Mr. BROWN. From the private sector?

Mr. BURROWS. That's correct.

Mr. BROWN. Mr. Burrows, there are some other questions that we would like to explore with you but I'm not going to take the time to do that. But if we send you some questions from the staff would you be kind enough to respond to them in whatever detail is necessary?

Mr. BURROWS. Yes, sir.

Mr. BROWN. Thank you very much.

Our next witness this morning is Dr. Robert L. Brotzman who is the Assistant Director for Computer Security at the NSA. That's a very high level position, isn't it, Dr. Brotzman, indicating the importance of computer security.

Mr. BROTZMAN. Mr. Chairman, the Director, Lincoln Farr, made that an assistant directorship a little over a year ago.

Mr. BROWN. We are pleased to have you here and hope you can shed some light on the need for this congressional initiative and we look forward to your testimony, which will be placed in the record in full.

STATEMENT OF ROBERT L. BROTZMAN, ASSISTANT DIRECTOR FOR COMPUTER SECURITY, COMPUTER SECURITY CENTER, NATIONAL SECURITY AGENCY

Mr. BROTZMAN. Thank you, Mr. Chairman. My name is Robert Brotzman and I serve as an Assistant Director at the National Security Agency for Computer Security, and also the Director of the National Computer Security Center. Thank you for the opportunity to testify on H.R. 2889, the Computer Security Research and Training Act of 1985, and to address the Government's capacity for performing research and training activities in computer security.

I'd like to discuss why the Government's present computer security structure, supported by the National Security Decision Directive 145, represents the best approach to providing computer security research and training and why, therefore, we must oppose H.R. 2889.

Raising computer security awareness across the entire Government and providing the training needed for managers, computer operations professionals, computer users and education specialists is an enormous undertaking.

The National Computer Security Center has prepared a plan for providing this training and initial contacts have been made with the Civil Defense agencies encouraging civil and defense agencies—encouraging their participation in the planning and execution of this task.

The plan was developed under NSDD-145 direction that technical assistance and other related services of common concern be provided to departments and agencies of the Government where ap-

BEST COPY AVAILABLE

propriate, and where appropriate, to private institutions. This effort will be greatly bolstered if, as I expect, the National Telecommunications and Information Systems Security Committee issues a national policy that makes education and training in all Federal departments and agencies mandatory.

Training and awareness are high priorities of the Computer Security Center. Other priority efforts well underway are a Vulnerability Reporting and Detection Program and a Research and Development Program. Both of these efforts are essential to a properly formulated training program.

Until the signing of NSDD-145, the Center's activities were aimed at ensuring the security of data being processed by DOD computers. However, the majority of our programs can be and are being geared to the needs of the civil sector, and in some cases, to the private sector.

For example, I have no doubt that our Vulnerability Reporting Program will, with minor modifications, serve the rest of the Government equally well. We've created a structure through which vulnerabilities discovered within specific systems are to be reported to a central point. The vulnerability information and the best remedial action will be shared with other users of the vulnerable component.

The benefit to be realized from such a centralized system is substantial. Vulnerability data is used to plug holes. It also improves our knowledge of the weaknesses and strengths of computer systems, and that knowledge will help guide and shape our training and awareness programs; programs that are now being geared to a Governmentwide audience.

We fully realize that such an audience is much too large to be served by the Center alone or for that matter, by any organization working alone. We think in terms of a national level effort to insure that each Government organization has adequte computer security education and awareness programs. These could include full-fledged courses developed and conducted inhouse by large agencies; for smaller agencies, awareness programs and dependence on other sources for formal courses; and for even smaller ones, relying totally on other government training organizations. The Department of Energy is a good example of a large organization with an established, successful program.

Before going on to research and development, I'd like to mention that I have entered in my written testimony descriptions of some of the Center's more recent accomplishments in training and awareness. In fact, as we meet here this morning, a conference is going on at Fort Meade, that both Jim Burrows and I would be attending but not for the honor of speaking before you, that involves about 36 organizations of government, all of whom are professional trainers.

Mr. BROWN. If it weren't for the honor, you'd just as soon be out there. [Laughter.]

Mr. BROTZMAN. Not really, sir. The R&D program is challenging, and our greatest challenge lies in converting research results into marketable security products. The approach we have taken is to divide our effort into five distinct areas, and each of these subprograms which comprise the Consolidated Computer Security Program, explores particular aspects of computer security research

BEST COPY AVAILABLE

and development. Most are distinct from research areas pursued at the National Bureau of Standards; however, in some areas, the work of the Center and the work of NBS are complementary and we regularly consult.

In virtually all of the activities that I have mentioned we have relied the support and cooperation of other government agencies, and we in turn really support many of them. We have had and will continue to have a close, highly beneficial working relationship with the National Bureau of Standards. We have not yet encountered disagreements concerning areas of responsibility.

Functions that seem to overlap we address together, and very effectively, I might add. Tasks clearly in the purview of one are often attacked with the help of the other. The responsibilities with which NBS is currently tasked; responsibilities which in my opinion they impressively fulfill, do not conflict with but rather complement those assigned to the National Computer Security Center.

The active role taken by NBS in the NTISSC's Subcommittee on Automated Information Systems Security will insure that those responsibilities continue and that any potential duplication of effort is quickly identified. You may be aware that Mr. Burrows chairs a working group of that subcommittee.

I see absolutely no erosion of the NBS role in computer security resulting from the implementation of NSDD-145. Existing programs at the Center and at NBS are generating effective momentum under the current NSDD structure. I would not want to lose this momentum. Programs to get the security job done are in place, and a cooperative effort is underway to attack and solve the computer security problem facing the Government and the private sector.

To summarize, the Government has the structure to do the computer security education and the computer vulnerability research that is needed. We plan to work closely with other government departments, as we do in our other endeavors where we depend heavily on the cooperative efforts of highly capable organizations such as the Bureau. The program is established and the effort has begun.

While we applaud the goals of H.R. 2889, we believe that the executive branch activities that are underway can fulfill these goals. What all of us are trying to do is too important and time critical to allow for the delays of regrouping. The technological disasters we're trying to avert are very real. We have to get on with the job, and with your committee as an ally, I'm sure we can get the job done. Thank you, Mr. Chairman.

Mr. BROWN. You skipped over a lot of stuff you have in here.

Mr. BROTZMAN. Yes, sir. Only in the interest of brevity.

Mr. BROWN. All right. Mr. Lewis, do you want to start some questions?

Mr. LEWIS. Thank you, Mr. Chairman.

How would you say H.R. 2889 affects your ongoing programs at the Computer Center? How would it affect it?

Mr. BROTZMAN. Probably it would cause a delay while we figured out exactly what the roles would shake out to be. The latest version that I have seen was from late last week, I believe, and that would have a substantial effect, if I correctly interpret them. I be-

BEST COPY AVAILABLE

lieve the word "exclusive" showed up in the wording of the last bill I saw. I think it would upset the apple cart.

Mr. LEWIS. How will H.R. 2889, both the original and as amended, affect NSDD-145 and NTISSC activities?

Mr. BROTZMAN. As originally structured, sir, I couldn't see there was a great effect. As it was amended, it looks to me like a rewrite of NSDD-145 into law, only under Commerce as opposed to the lead being Defense. I think that would be a substantial change.

Mr. LEWIS. Critics of NSDD-145 have asserted that NTISSC is overly represented by the military. Have the civil agencies expressed dissatisfaction with the current makeup?

Mr. BROTZMAN. Sir, that is an unusual situation. I hear the dissatisfaction referred to and yet I have personally never heard any from a civil organization. I have never seen a vote taken within the subcommittee or committee structure that went along civil/military lines, nor have I personally heard criticism from a member or a nonmember of that structure that was of substance; that is, something was happening or not happening that affected them.

Mr. LEWIS. Have you heard any comments that consideration should be given to enlarging or altering the committee to increase the civil makeup?

Mr. BROTZMAN. Yes, that has been discussed. Within the subcommittee that I chair, we discussed that at our last meeting. The subcommittee indicated that I should go forth and discuss that with several large computer using organizations of Government not now represented.

The problem being, of course, that our concerns are with national security related information. It is not altogether clear that some of the larger computer users in Government really have data that needs protection for national security reasons.

Mr. LEWIS. Do you feel that NSDD-145 conflicts with the Brooks Act?

Mr. BROTZMAN. No, I don't.

Mr. LEWIS. You do not. Thank you. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Walgren?

Mr. WALGREN. Thank you, Mr. Chairman.

In your testimony you indicate that I gather as a first step, you have sent letters to the heads of 79 organizations, and that 14 have responded. You visited those 14 at this point.[1] One of those is the Department of Health and Human Services.

Yet, as I understand it, the inspector general of Health and Human Services was testifying here yesterday that he is the one most interested in pushing computer security and he had not had any contact with or direct awareness of your involvement with HHS.

I guess the question is, if the strongest advocate of such an effort in an agency is not really involved with your program yet, is the program contact effective?

Mr. BROTZMAN. I cannot address how things were handled within HHS. The letters that I sent went to the head of the organizations of Government. If they named the point of contact, it was that

[1] Sixty-eight organizations have responded to the Computer Security Center's letters and 14 organizations were visited during the month of October.

BEST COPY AVAILABLE

point of contact that my staff visited. If Mr. Kusserow was not so named, I am not surprised that he may not be aware of it.

Mr. WALGREN. I gather that the contact with these civilian agencies is fledgling at best at this point. Perhaps a point contact as opposed to any kind of indepth working relationship of any kind.

Mr. BROTZMAN. The letters just went out this summer. I believe they were dated in August.

Mr. WALGREN. How big an effort is this? What is your budget?

Mr. BROTZMAN. My budget is——

Mr. BROWN. If you will allow me, his budget may be a lot bigger than what we are interested in. I would like to clarify that we are talking about security, training and related things that you have discussed here, not all the research that you may be involved with.

Mr. BROTZMAN. My budget is not broken out that way. I would be happy to provide the full budget details to the committee in writing.

Mr. WALGREN. You talk in here about limitations or how big the problem is and how it has to be addressed piecemeal and it has to be addressed in each individual agency.

Without having to be specific about numbers, could you give us an estimate of what you feel the resources needed to address that problem effectively are?

Mr. BROTZMAN. I am less able to give you answers on resource requirements but I can give you some answers as to the number of people involved.

Mr. WALGREN. In this specific function which Mr. Brown focuses on?

Mr. BROTZMAN. The target population within the executive branch, the military services, the legislative and judicial branches, of people in need of training and awareness, comes to roughly $4.8 million. That is my estimate. Excuse me, 4.8 million people. It is a very large crowd of people.

Merely every manager in Government these days is supported by automatic data processing systems. Without an awareness of the dangers that are inherent in such systems, we believe he can't do his job effectively.

Mr. WALGREN. That is such a big pill.

You indicated in your testimony that the audience is much too large to be served by the Center alone, or for that matter, any organization working alone, and therefore, it is not useful to talk about national programs for education and awareness, rather we must talk about, I gather, to go back to your text, a national level effort within—to ensure that each organization within the Federal Government has adequate computer security.

What I am trying to raise is on the one hand I hear you saying, look, we have this one organization and we are trying to address this problem, and you don't want to regroup because time might be lost. Yet, you say the very thing that we need is what this bill that you oppose calls for, which is an effort located within each agency that is designed to develop this sensitivity and awareness.

It seems to me when you say it is much too large a problem for the Center alone and you need an effort within each agency, that this bill would be just what the doctor ordered. Yet, you are opposed to it.

BEST COPY AVAILABLE

Mr. BROTZMAN. The argument, I believe, is if one views it as giving a charter to someone in Government to go train all in Government, I believe that would be a mistake. I don't think that is what is needed. What is needed is a central orchestration to help people help themselves. I think that is what is going on at Fort Meade today, with 75 trainers throughout Government who are there trying to figure out what they can use of each other's programs, to help each other understand what others have done, to help them shape their own programs.

The sharing aspect within Government, I think, is very much called for.

Mr. WALGREN. Should we not be requiring each of them to help themselves? Given the limited resources that these agencies are dealing with, unless we force the priority on the issue, it may very well be that the effort will be diverted to some other pressing need.

Should we not require by legislation each agency to address this problem?

Mr. BROTZMAN. I don't know how to answer that one very well, in that sometimes people are told what to do and for reasons do not do it. Sometimes they don't know how. Sometimes they can't afford it. I think the effort to require that is now underway with the existing structure.

My subcommittee reported out a recommendation to the parent committee that such training and awareness programs be mandatory. If the national committee approves of that and it goes for signature to the executive agency of the Government, my understanding of NSDD-145 is that would be required.

Mr. WALGREN. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Boehlert.

Mr. BOEHLERT. Thank you, Mr. Chairman.

If I hear you correctly, you are saying, and you said it at the end of your testimony, that the Government, under the existing legislation, has the structure that we need to do the job that needs to be done, and if I am further hearing you correctly, you are saying basically we have the resources to do it.

What is really needed is the coordination and commitment. That word "commitment" keeps coming back to me all the time.

I have the feeling that in the defense sector, we are kind of concerned about computer security, and a lot of people are buzzing about doing something about it, but in the civil sector, people at the top are just yawning when you mention the subject, and are more directed toward other activities.

Is that a correct interpretation of what you are telling me? Forget about the yawning part.

Mr. BROTZMAN. Let me see if I can answer that somewhat.

Mr. BOEHLERT. Let's start with the structure first. Do you think the existing structure is sufficient to do what needs to be done?

Mr. BROTZMAN. I believe the tools are all in place to allow us to solve this problem. I see no great lack right now.

Mr. BOEHLERT. Which is kind of encouraging because most of us are in the habit of running home and telling people about all the new laws we have passed. I sometimes think we would be better off if we came back home and said "we didn't pass this one, this one, and this one." I think the people would applaud a little bit more.

BEST COPY AVAILABLE

What about the resources? Everybody wants more money. We understand that. Essentially under the existing budgetary constraints, do you really think we have the resources required to do the job, if we also have the commitment on the part of all the principal players and if we have the proper coordination, two things that I think are lacking?

Mr. BROTZMAN. The knowledge base that we have now will support an effective training program, and it will support the substantial improvement in the security of computer systems operated by and for the U.S. Government.

The area that is not well addressed in the resources sense yet has to do with advancing the state of knowledge well beyond what we know how to do now.

The program that we in the center are on, I describe as a three prong program. The first prong of that is to do immediately those things we already know how to do, and that is where the commitment comes in. We have to demonstrate that we are serious and go do it. That has to do with the vendors making available to customers, both private and public, systems with far better security attributes than are now on the market. The vendor community knows how to build them. I believe they will build them when they detect we are serious about using them. It is not a great expense item either.

The second prong has to do with making available substantially enhanced technical capabilities of computers. We think that can be done by the end of the decade. Once again, it is technology that is known. Building such systems, a little more expensive, and the community of users will probably be smaller, roughly half of the previous community.

The third major thrust has to do with making a fairly substantial national commitment to learning how to do the job right. We really don't know how to do it right. We have a multi-hundred billion dollar a year industry that was built on the driving forces of more capacity, more capability. I think it is time that we now add the third driving function, which is make it exhibit some security and integrity.

Mr. BOEHLERT. Thank you very much. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Brotzman, I am really very impressed with your presentation and description of your program. I think it is a model for what could be done.

Part of the problem may be that it originates in a Defense Department agency and one of the more secretative Department agencies. Most of the members of Congress do not get an opportunity to know what is going on over there. Of course, every member of Congress wants to know everything that is going on everywhere. [Laughter.]

Mr. BROWN. It may cause problems as a result of that.

To what degree do you have your program reviewed and an oversight by appropriate committees of Congress? Does the Armed Services Committee or other committees play an active role in giving guidance or giving trouble to the agency with regard to this computer security problem?

Mr. BROTZMAN. The committee structure within Congress which examines the budget is roughly the defense appropriations struc-

BEST COPY AVAILABLE

ture and the intelligence community structure. We have no intelligence role within the center but because we are a subordinate organization of NSA, we sort of naturally go under their perview.

The scrutiny is clearly there by both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

As for specific guidance of do this or don't do that, I personally do not recall any, which I take to mean that they view the program to be appropriate.

Mr. BROWN. You haven't had any fundamental problem comparable to the NBS with regard to Congress making major cutbacks or restrictions in your budget for this activity?

Mr. BROTZMAN. No, sir.

Mr. BROWN. You are one of the fortunate ones.

Mr. BROTZMAN. If one measures the gap between what you ask for and what you get, then I am one of the unfortunate ones.

Mr. BROWN. You mean you asked for even more than what you got?

Mr. BROTZMAN. Yes, sir.

Mr. BROWN. I note with interest the program you describe as the computer security vulnerability reporting program. I at one point had some familiarity with what seems to be a similar program available to defense contractors for a materials defects reporting program. You may not be familiar with it. There was a central data bank in which all Government contractors could report materials failure that might have an impact and to some degree, materials and components which failed, which might have an impact on other contractors. That was available on a fairly wide basis to anyone who might need that kind of information.

May I assume that this program that you are describing here is of a similar nature, that it would be available to all interested parties, assuming there were no classification problems or things of that sort with regard to computer failures in security?

Mr. BROTZMAN. I intend to offer the program outside of defense, sir. Within defense, I expect that any day now it will become mandatory. The Secretary is sufficiently concerned about those vulnerabilities.

Mr. BROWN. Within defense, there would be a mandatory reporting program?

Mr. BROTZMAN. Yes, sir.

Mr. BROWN. The data bank could be accessed by other parts of the Defense Department?

Mr. BROTZMAN. As you can well imagine, the delicacy of the control problem with such data is severe. The current plan says that there will be no outside access. It will always be through a human being. I intend to keep the number of human beings who have access to the full data base to the absolute minimum.

I think data like that is clearly dynamite, insomuch as it tells you specifically how to defeat the safeguard mechanisms of systems.

Mr. BROWN. Yes, I would be very interested in it myself.

To what degree would it be possible for State and local governments—many, in many cases, operating Federal programs, and we had testimony yesterday, for example, on the Food Stamp Program

BEST COPY AVAILABLE

which is a multibillion-dollar program, subject to all sorts of fraud and abuse through computer manipulations—to what extent would these kinds of programs have access to the kinds of information that you are generating, including the training programs and other things of that sort?

Mr. BROTZMAN. As long as it is a member of the Federal Government who needs the information for the protection of national security-related data, or a member of the private sector who has such data that it's in the national interest to protect, I am clearly directed to provide that assistance to the extent that I can.

For those that fall outside that arena, I guess we are very much in the role of we'd like to do somebody a favor but the authority to do so, especially if it involved expenditure of Government funds, is not there.

Mr. BROWN. But you do have this road show that you described, and you have modules of training programs and so on, and you have indicated I think that this would be available to universities and others conducting training programs, and presumably you would not put any restrictions on making that available to anyone who would benefit from it.

Mr. BROTZMAN. The university involvement is, if you will, a selfish interest on the part of the government. We very much want to have the universities begin curricula in computer security as well as computer science, and for that reason we heavily involved, or we intend to heavily involve the universities.

Mr. BROWN. So there should be considerable diffusion of that kind of basic information, if not directly between you and with, say, a State or local government, then from you to the universities and their training and education activities and then to the proper people in State and local government.

Mr. BROTZMAN. If I understand the thrust of your concern, sir, I believe that the programs developed to protect the national security-related information will be of benefit to all who have data that they wish to protect from either unauthorized reading, unauthorized manipulation or for denial of service or for disruption of operations.

Mr. BROWN. There's a very important national security area that I understand you have looked at, and that's the problem of election manipulation. Do you see that as a national security problem?

Mr. BROTZMAN. The national security-related terminology is not fully defined yet. I think it's clear that that is fundamental to our form of government, that such things have integrity.

Mr. BROWN. Well, that is one of the most widespread uses of computers, at least during the election period. Could you describe the kind of relationship or the kind of activity that you have had in connection with the development of more secure processes for guaranteeing the validity of election returns? We sometimes wrestle with that problem right here in Congress.

Mr. BROTZMAN. We have taken no overt action specifically related to improving the security or integrity of election results. What we did was stimulated this summer largely by a couple of New York Times articles, I asked one or two people in the Center to find out what the technical vulnerabilities were, for several reasons. We want to understand technically how such subversion could take

BEST COPY AVAILABLE

place. We also want to be able to raise people's awareness about how much we trust computers without really thinking about it.

Mr. BROWN. And you see no reason why you couldn't continue to examine that problem and at least analyze the possibilities that systems might be faulty and find ways of correcting that?

Mr. BROTZMAN. That is correct.

Mr. BROWN. I don't have any further questions immediately. Does any other member wish to pursue additional questions?

Mr. LEWIS. Mr. Chairman, I would like to raise one question with Dr. Brotzman. When we talk about security, we can get at odds with the need for privacy in the computer, and I guess if we solve the communications and computer security problem is the derivative effect to increase privacy?

Mr. BROTZMAN. I believe so, yes.

Mr. LEWIS. What is the privacy concern that's not being addressed by the Government at this point? Do you know?

Mr. BROTZMAN. Well——

Mr. LEWIS. Or shouldn't I have asked that question?

Mr. BROTZMAN. I'm trying to think of how to answer that one without just muddying the waters. In general, when you have systems operated by and for the Government that have inadequate security build into them, then any data that goes into such computers can be gotten at through the back door, not just the front door. When that data involves me or you as private citizens, I think we're highly offended that that could take place. And for that privacy reason alone, I would very much like to see the computers in the Government be much more secure.

Mr. LEWIS. Thank you.

Mr. WALGREN. Mr. Chairman, if the committee would permit, do you see any difficulty in having the military or security-related agencies developing such a comprehensive network of contact and access to information across the range of the Government? Is there any reason at all to be feeling that our general instinct of civilian control of the military would want us to at least invert the order of involvement? If that communicates.

Mr. BROTZMAN. I am familiar with that concern. I don't believe there's much substance behind it in the sense that the NSDD structure doesn't give the defense community control of civil community or private community data. It puts them in a leadership role to help develop and make available to all of us better techniques and, if you will, better computers in the security dimension. So I think that works to all of our good.

The Defense Department doesn't control civil sector data, no. The civil sector will control its own data.

Mr. WALGREN. I see. Thank you, Mr. Chairman.

Mr. BROWN. Dr. Brotzman, we may want to have you answer a few more questions in writing, if you don't mind. If you will promise to do that, we will excuse you so you can get back over to your program.

Mr. BROTZMAN. I'd be most delighted.

Mr. BROWN. Thank you very much. It is, I think, the general feelings of the committee members that you have been an outstanding witness and you've helped us a great deal—even if we

55-930 0 - 86 - 6

BEST COPY AVAILABLE

don't want the Defense Department running all of our computer security systems.

[Prepared statement of Mr. Brotzman follows:]

BEST COPY AVAILABLE

Statement of Robert L. Brotzman, Director, National Computer Security Center

Mr. Chairman and Members of the Subcommittees:

Thank you for this opportunity to testify on H.R. 2889, the Computer Security Research and Training Act of 1985, and to address the government's capacity for carrying out computer security research and training activities. I would like to discuss how the computer security structure for protecting national security related information established by National Security Decision Directive 145 (NSDD 145), assists in providing computer security research and training for federal agencies. We have a number of activities underway that we believe, along with activities in other agencies, are addressing the concern that prompted H.R. 2889. Therefore, we oppose H.R. 2889; we also oppose the recently amended version of the bill reported out by the Legislation and National Security Subcommittee of the House Government Affairs Committee.

As you know, NSDD 145 establishes the Executive Branch initiative to protect computer and communications systems which process information of concern to the national security. An important facet of such a program is its efforts to raise computer security awareness across the entire government and providing training needed for the managers, computer operations professionals, and computer users. Therefore, one of the Center's highest priorities is the building of strong training and awareness programs. Other efforts well under way include research and development, and vulnerability detection and reporting. Accurate information on computer vulnerabilities is a necessary prerequisite to a properly formulated training program. An aggressive research and development effort bolsters training as it provides the solutions to what I have described in the past as the curse that comes with the blessings of automation.

Until the signing of NSDD 145, the Center's activities were aimed at ensuring the security of data being processed by DoD computers. NSDD 145 expanded the Center's role to assist with government-wide protection of national security information. Many of our tools can be, and are being, adapted to be useful to civil agencies and in some cases to the private sector. For example, I have no doubt that the Computer Security Vulnerability Reporting Program being developed by the Center for DoD systems would, with minor modification, serve the rest of the government equally well. We have created the structure through which vulnerabilities discovered within specific systems are reported to a central point. Some vulnerabilities are system-unique; but, whenever the weakness is found to be in an operating system, in a generalized software module, or in the hardware used in multiple systems, the vulnerability information and the best remedial action would be very useful information for all users of the faulty component.

BEST COPY AVAILABLE

In addition, information collected on vulnerabilities will also improve our knowledge of the weaknesses and strengths of computer systems, and that knowledge will be used to help guide and shape our training and awareness programs--programs that are also being adapted to be more useful to a government-wide audience.

For protecting national security information, the Center has developed a National Computer Security Education Plan. It implements NSDD 145 direction that "technical security material, other technical assistance, and other related services of common concern," as required to accomplish the objectives of the Directive, are to be provided to "departments and agencies of the government and, where appropriate, to private institutions (including government contractors)."

We fully realize that the audience concerned with protecting national security information is much too large to be served by the Center alone, or for that matter by any organization working alone. The immense size and diversity of functions performed in government suggest that it is not very useful to talk about national programs for education and awareness. Rather, we must think in terms of a national-level effort to ensure that each organization within the federal government has adequate computer security education and awareness programs. From our perspective such programs should incorporate special needs for protecting national security information. For large agencies, this may mean a full-fledged program with courses developed and conducted in-house. Smaller agencies may have only an awareness program and rely on other sources for formal courses. For example, some organizations, such as the Department of Energy, already have active, successful education and awareness programs established. However, other organizations, especially smaller ones, are looking to government training organizations to provide the formal courses and more tailored training sessions. The DoD Computer Institute, the Office of Personnel Management, and the Computer Security Center, all include computer security courses in their curricula. Computer security courses are also available at some academic institutions. And there are numerous courses available from the private sector: from firms that provide them for profit, and from non-profit organizations such as professional societies.

As I mentioned earlier, the educational services of the Center focus on protecting national security information. They are directed toward four groups: the general user of computer systems; managers of computer systems; education specialists; and computer science people who require specialized training.

BEST COPY AVAILABLE

In general, our program is geared toward (1) developing state-of-the-art computer security education modules and making them available to those who need them, (2) assisting others in setting up programs, and (3) acting as a clearinghouse for available information.

I would like to outline some of our specific recent accomplishments in education and awareness.

We offer a National-level course for managers that provides a general introduction to the national security need for computer security and what can be or is being done to provide it.

We offer a course on advances in computer security R&D for personnel from throughout the government. This week-long course gives computer science professionals a firm basis for understanding how to implement security. We have held other technically oriented courses in artificial intelligence, verification tools, and software-oriented computer architecture.

We have developed the first five modules for what we call our "road show." This is a training session tailored to a specific organization. The roadshow is a multi-media approach to providing information on computer security to an organization at its site. With instructional modules, the roadshow can range from a 1-hour to a several-day presentation, covering topics such as the threat to information in computers, risk assessment, standards for evaluating security, and software and hardware available to improve security.

Our awareness activities include an industrial symposium, held last spring; awareness posters, which are distributed to a broad spectrum of government agencies; and two awareness video tapes (we have distributed nearly 600 copies of these since this June).

One activity that we hope will have strong impact on education and awareness is a symposium that we are sponsoring, and which is being held today, for computer security educators in the federal government. We are meeting to learn about each others' programs and to discuss how we can help each other, especially in sharing resources such as course materials. We intend to make this an annual event, and expect it to increase in attendance and length from this year's first effort.

In support of what we see as our role as an information clearinghouse, we are in the process of setting up several data bases on computer security education-related information. Listings from the data bases will be given broad distribution. The first data base is on educational activities. It will include courses,

BEST COPY AVAILABLE

workshops, and seminars offered by government agencies, by academic institutions, and by the private sector. The data base is nationwide in scope.

In FY 86, we will continue the existing courses, develop ten more modules for our roadshow, produce three more video tapes, and publish a handbook describing how to set up an awareness program.

By next spring, we hope to have a data base on upcoming conventions and conferences, and one on computer security education and awareness products.

In all our education and awareness activities at the Center, we follow a philosophy of openness and sharing. All the education and training material that we develop is available to other organizations. We are trying to "package" our resources to ease this sharing. Often the information can be shared at little or no cost to the receiving agency. For example, to receive a copy of our video tapes, we ask only that we be sent a blank tape.

Through an academic outreach program, our education and training people have been assisting the academic community in getting computer security into computer science courses. A spring conference is planned for further discussions with academicians on this subject. We also will be encouraging the inclusion of computer security awareness in management courses. Educational institutions, both government and private, are recognizing that managers need to be "computer literate." We believe that being literate must include an appreciation of security requirements.

During FY 86, we will begin our own entry-level training program. This program will be a mix of courses, video's, reading, and discussion groups that together will teach our incoming Center personnel what they need to know about computer security. There are "tracks" for nine different kinds of employees--from clerical persons to managers to system evaluators. The modules that make up this program, like those in our roadshow, will be available to any requesting organization. We are packaging our modules so that they are complete and ready for use--scripts, graphics, exercises, video's--whatever is needed by a particular organization.

We have published, or in some cases are preparing for publication, computer product evaluation criteria, guidelines for applying certain levels of security in specific environments, and guidance on subjects such as audit, discretionary access control, office automation, data remanence, and data base management. Many of these publications may be adaptable by the civil agencies to assist in securing other sensitive information.

BEST COPY AVAILABLE

Let me single out one of the several areas in which we have been dealing with civil sector elements of the government. This past August, letters were sent to the heads of 79 organizations in the Legislative and Executive Branches, independent government establishments, and government corporations, offering computer security assistance, outlining the services offered by the Center, and requesting a point of contact for computer security matters. A team has been formed to introduce these organizations to the Center's mission, discuss the need to protect sensitive national security data, and make them aware of the security measures available to protect this data.

The response has been extremely enthusiastic. Last month alone the team visited 14 government organizations in the civil sector, all of whom were very receptive to what we had to say. These visits were made to the Department of Agriculture; Department of the Treasury; Office of Technology Assessment; Department of Labor; Department of Commerce; Farm Credit Administration; Department of Transportation; National Aeronautics and Space Administration; Department of Education; Veterans Administration; Department of the Interior; Department of Justice; Department of Health and Human Services; and the Office of Personnel Management. The list is growing, and the team will be busy for some time.

The R&D program for tools to protect national security information is challenging. Our greatest challenge lies in converting research breakthroughs into marketable security products. The approach we have taken is to divide our efforts into five distinct areas: secure computer system architecture, secure data base management systems (DBMS's), aids to evaluation, modeling and verification, and network security. Each of these subprograms, which comprise the Consolidated Computer Security Program (CCSP), explores particular aspects of computer security R&D. Efforts under the CCSP are closely coordinated with NBS. Most of these subprograms are distinct from research areas pursued at NBS; however, in some areas, the work of the Center and NBS is complementary. Complementary R&D efforts by the Center and NBS are ongoing or planned in the areas of developing risk analysis methodology; evaluating limited-function security products; participating in network security methodology; and evaluating criteria development and network security protocols. The Center and NBS regularly seek each other's technical assistance in these matters.

The responsibilities with which NBS is currently tasked--responsibilities which, in my opinion they impressively fulfill, do not conflict but rather complement those assigned to the National Computer Security Center under NSDD 145. As you know, NBS promulgates federal standards and guidelines as well as provides technical assistance to federal agencies in all areas of computer usage, including security of computer systems. The

BEST COPY AVAILABLE

National Computer Security Center is focused on protecting national security information. The active role taken by NBS in the NTISSC's Subcommittee on Automated Information Systems Security ensures that any potential duplication of effort is quickly identified and avoided. I see absolutely no erosion of the NBS role in computer security resulting from the implementation of NSDD 145. Existing programs at the Center and at NBS are generating effective momentum. I would not want to lose this momentum. Programs to get the computer security job done are in place and a cooperative effort is underway to attack and solve the computer security problem facing the government and private sector.

In virtually all of the activities I have mentioned we have relied on the support and cooperation of other government agencies, and we, in turn, freely support many of them, among the closest of which is NBS. We have had and will continue to have a close working arrangement that is highly beneficial to both parties. We have not yet encountered any subjects of disagreement concerning areas of responsibility. Functions that may seem to overlap we address together--very effectively I might add. Tasks clearly in the purview of one are often attacked with the help of the other.

Perhaps the best-known manifestation of this cooperation is the annual Computer Security Conference, which has been cosponsored by the Center and NBS for the past eight years. Early this month, 950 people from 100 defense, civil, and private organizations gathered to discuss problems and accomplishments, and to exchange ideas. This number is double that of 1983, and includes 55 representatives of 8 nations on 4 continents. We share with NBS the satisfaction that comes with seeing the long-ignored subject of computer security draw such rapidly growing interest.

To summarize, the government has the structure to do the computer security education and computer vulnerability research that is needed. We plan to work closely with other government departments, as we do in most of our endeavors, where we depend heavily on the cooperative efforts of highly capable organizations such as the National Bureau of Standards. The program is in place and the effort has begun. While we applaud the goals of H.R. 2889, we believe Executive activities underway will fulfill that goal.

What all of us are trying to do is too important and time-critical to allow for delays and regrouping. I assure you that your concerns are my concerns. The technological disasters we are trying to avert are very real. We have to get on with the job, and with your committee as an ally, I am sure we can get the job done.

BEST COPY AVAILABLE

ROBERT L. BROTZMAN

Assistant Director of NSA for Computer Security
Director, National Computer Security Center
Chairman, Subcommittee on Automated Information System Security

Dr. Brotzman was born in Kamiah, Idaho on October 8, 1938. He served in the United States Air Force Security Service from 1956 to 1960, with assignments in Korea, Japan, and the U.S. He then attended the University of Wisconsin and the Ohio State University. He was selected as a National Science Foundation Fellow in 1964, and in 1965 graduated at the head of his Engineering class with a B.E.E. (summa cum laude) and a M.Sc. In 1968 he was awarded a Ph.D. in Electrical Engineering from Ohio State. Honors included selection by Tau Beta Pi, and Eta Kappa Nu, plus the President's Scholarship Award for 1964 and 1965.

Dr. Brotzman joined the National Security Agency in 1966, having worked on NSA contracts on linguistic research through the Ohio State University Research Foundation. His assignments at NSA have included speech research in the Office of Research and Engineering, a series of assignments in the National Cryptologic School where he served as Assistant for Engineering Sciences, Chief of the Computer Sciences Division, Head of the Department of Sciences, and finally, Dean of the Science and Technology Faculty. Dr. Brotzman returned to the Research and Engineering Directorate in 1973 as the Chief of the Special Systems Division and then joined the Operations Directorate in 1975 as the Chief of the Signals Analysis Division. Other assignments in operations included Chief, and Special Assistant to the Chief of an Operations Group. In July of 1984 he returned from a two-year field assignment as a Chief of Station to become the Director of the Computer Security Center, and an Assistant Director of the National Security Agency. In November of 1984 he was named Chairman of the Subcommittee on Automated Information Systems Security of the National Telecommunications and Information Systems Security Committee.

As Director of the Computer Security Center, Dr. Brotzman is responsible for providing technical support in computer security, developing technical criteria, evaluating commercial software and hardware systems for applicability, performing selected evaluations of computer systems, conducting and sponsoring verification and analysis tools, conducting training, and disseminating computer security information throughout the Federal government.

He is married to the former Darlene Nelson of River Falls, Wisconsin. The Brotzmans have three daughters, Laura, Lisa, and Michelle ranging in age from 22 to 25, and a grandson, Justin Michael Bolster born in December 1984.

BEST COPY AVAILABLE

Testimony of Donn B. Parker Before the U.S. House of Representatives, Subcommittees on Transportation, Aviation, and Materials, and Science, Research, and Technology, on H.R. 2889, The Computer Security Research and Training Act of 1985, on October 30, 1985

H.R. 2889, Computer Security Research and Training Act of 1985, promotes and supports security in exactly the right functional direction. While I don't feel expert or knowledgeable enough to comment on how it should be implemented among the various government agencies, I have recommendations for the subjects it addresses, its impact, and the security needs in the private sector.

While many of those who have testified on H.R. 2889 have indicated that it is superfluous, I find that an extension of its intent and function would make it important legislation to meet the government's needs for adequate information security that are not now being met. Specifically, solutions to two problems--lack of information security, and awareness and motivation for good security among trusted people using sensitive information and computers--can be advanced by extending H.R. 2889.

My recommendations are thus to:

1. Extend the scope of the bill to all information in all forms and media without regard to technical means for creation, processing, communication, or storage.

2. Extend the requirement for information security education, awareness, and motivation to all information workers along with application of appropriate awards and penalties.

3. Provide for development of descriptions of sensitive information, code of conduct, policies, and job performance reviews that hold government workers accountable as managers, users, or custodians for the security of sensitive information in their charge.

4. Specify that confidential employee advisory services for personal problems be made available to trusted information workers.

BEST COPY AVAILABLE

5. Establish the requirement for specialized education of computer security officers and plant or building security officers, the former in security and intelligence skills as well as technical skills and the latter in technical skills by a process of cross-training.

6. Stress the need for multiple, parallel, and independent information security research in several government agencies to be more assured of comprehensive identification of vulnerabilities and solutions.

Discussing these suggestions in order--first, H.R. 2889 falls short in recognizing that the security of information, not just computers, is the more fundamental need. We are creating Maginot Lines when we concentrate our efforts on only technological protection of information in computers and communications. Predictions of the paperless society have not materialized. We have a non-paperless society today and are producing more sensitive information on paper than ever before with the use of millions of microcomputers, most having a high-speed printer attached. In addition, we are conveying more sensitive information orally than ever before, as computers are used to automate our work thus giving us more time to talk.

Thus, our problem today is information security, not just computer security, and in the future the need will probably be knowledge security as we start using expert computer systems with knowledge bases. After people, information and knowledge are the most important assets of business and government and must be protected in whatever form.

Second, the principal deficiency in computer security today is a lack of awareness of the need and motivation for good security among trusted employees. This deficiency is addressed in H.R. 2889 by Congressmen Glickman, Fuqua, Brooks, Brown, Wirth, Walgren, Nelson, Wyden, Hughes, Lewis, and Horton. My second, third, fourth, and fifth recommendations address this problem. I have found, in performing over 70 computer security reviews in the private sector over the past 16 years, that security is not effective until trusted employees are constrained by safeguards which they are willing to tolerate and support, since many such safeguards require extra effort beyond direct job productivity.

However, training and motivational efforts called for in the bill will not be effective unless there are accompanying rewards and penalties for recognized good and bad practices. A computer programmer can be sent to classes and made to read material, but he or she won't listen or respond unless self-interest exists. H.R. 2889 falls short in this regard.

BEST COPY AVAILABLE

Rewards for good security practices can include more favorable job performance and salary review evaluations, priority in office facilities and computer equipment usage, favored parking spaces, plaques, award ceremonies, and management recognition. Penalties can include adverse personnel file entries, reporting of poor practices to fellow workers, forced secret password changes, loss of privileges, and, in extreme cases, termination.

In businesses, I emphasize the need to confront information workers with clear and simple rules in policies, codes of conduct, and salary and performance reviews regarding authorized and unauthorized acts in automated workplaces. In such environments, the ethical standards of such acts may not be directly carried over from non-automated environments or from the informal computer environments of the past. Examples include personal use of computer time, copying and use of proprietary computer programs, and reading or harming others' computer data files. This confrontation is even more important with the explicit identification of authorized and unauthorized acts in new computer crime statutes.

I have interviewed over 50 so-called computer criminals and found that most of them had intense, unsharable problems that motivated their criminal acts. They saw themselves as problem solvers, not criminals. This finding has also been supported by much research in white collar crime. One conclusion from this is that information crime can be deterred to some extent by offering confidential help to trusted information workers with financial, alcohol, drug, gambling, social, workplace, and family problems.

An extremely important requirement for good information security is acquisition and use of intelligence concerning trusted employee aberrant behavior and activities. Most computer security officers and line managers whom I know are untrained in and unaware of this powerful security practice. Yet it is well known and practiced in many other security functions.

Computer security officers usually have computer technology backgrounds and don't understand the security profession. My own research for the Department of Justice and other recent studies indicate that the greatest threats to information and computers are from disgruntled trusted employees and employees with personal problems. Making line managers and technical security staff sensitive to detection of these problems on an informal basis and cultivating informal and formal informant networks are basic aspects of good security. Government intelligence services are expert in these security practices. They should provide this type of training to technical managers and computer security officers throughout government agencies where sensitive information is created, processed, stored, and communicated.

BEST COPY AVAILABLE

Training must include specialized courses for computer security officers in information and computer security subjects. The results will be more competent, cross-trained security staffs in both areas.

My sixth suggestion, for parallel research efforts, is supported as follows. At present, significant advances are being made in criminal law especially with legislation proposed by Congressman Bill Nelson and William J. Hughes, the Administration bill from the Department of Justice, and the current statute, Title 18, Chapter 47, Article 1030 of the U.S. Criminal Code. The best features of each combine well to meet the current needs.

Significant advances are also being made in technical computer safeguards as a result of the efforts of the National Bureau of Standards Institute of Computer Science and Technology and the new National Computer Security Center.

The evaluation of risks in government use of computers using comprehensive quantified risk assessment methods has been a failure and waste of valuable security staff resources. However, before a risk assessment is done, more focused use both of improved methodologies for important issues where adequate data are derivable and of a more practical baseline approach using many of the generally accepted and well-known product safeguards and practices (such as have been published by the National Computer Security Center, the National Bureau of Standards, and SRI International) can solve this problem.

Much of the security applied in the private, business, and non-military government sectors was first developed and used in the military and intelligence sectors. The use of identification badges, cryptography, and Tempest-conditioned equipment are examples. This transfer of security safeguards technology must be continued, and the National Computer Security Center and National Bureau of Standards are important mechanisms for that.

The private sector is becoming so dependent on concentrated, fragile, yet powerful information technology that national vulnerabilities are growing, as indicated in several impartial studies.* This situation justifies the national defense concerns identified in NSDD 145 and the expanded role of the Department of Defense. However, serious negative consequences must be avoided that could do more harm than good.

---

*Observations on the Resiliency of the U.S. Information Society. Rein Turn, et al. American Federation of Information Processing Societies, Arlington, Virgina. November, 1982.

BEST COPY AVAILABLE

Three issues are worthy of note in this regard. First, the profitability, productivity, and market shares must not be disturbed in harmful ways. Second, the private sector is international in its fundamental make-up. Foreign-owned and partly foreign-owned and multinational companies of national defense importance preclude an exclusive nationalistic approach. Third, it must be recognized that the vulnerabilities, enemies, and environments in the military are quite different in some respects from those in the non-military.

One potential solution is a mechanism developed in the private sector that was called for two years ago by the then head of the National Security Agency, Lt. Gen. Lincoln Faurer. One year ago, AT&T American Transtech joined with SRI International to begin development of the International Information Integrity Institute (a detailed description has been submitted to the subcommittee staff). I4, as it is called, would provide a conduit for information between the private sector and several pertinent government agencies, including the National Computer Security Center and National Bureau of Standards. It would promote good security practices in business and offer computer-related loss information on a timely basis. I hope to see I4 developed next year.

BEST COPY AVAILABLE

Mr. BROWN. Our next witness is Mr. Donn B. Parker, who is a senior management systems consultant with SRI International; a great organization.

We are happy to have you here this morning, Mr. Parker, and look forward to your testimony.

STATEMENT OF DONN B. PARKER, SENIOR MANAGEMENT SYSTEMS CONSULTANT, INFORMATION SYSTEMS MANAGEMENT DEPARTMENT, SRI INTERNATIONAL

Mr. PARKER. Thank you, sir. My name is Donn Parker, I am a senior management systems consultant at SRI International in California. By way of expertise, I have been in the computer field for 32 years, programming and managing computer centers in the private sector. The last 16 years I have spent doing definitive research on computer crime and information security. I have interviewed over 50 so-called computer criminals, and worked primarily in consulting in the private sector, but my work on the research side has been funded by the National Science Foundation, National Bureau of Standards, Department of Justice, and the DOD.

My statements here today are my own and not those of my employer or any of my clients, and I wish to have my written testimony accepted as read.

Mr. BROWN. Without objection, the full text will appear in the record, Mr. Parker.

Mr. PARKER. Thank you. I have seven points, including six recommendations. First of all, I believe that 2889 needs significant changes made in it, and particularly, concerning its scope.

The asset that we're trying to protect is not computers, but information. In the private sector in corporations, information is now thought of as a basic asset of business and needs to be protected.

Therefore, I believe that this type of legislation should focus on information and information security, to replace the old concept of just computer or telecommunications security.

A few years ago, there were estimates that today we would be in the paperless society, and just exactly the opposite has happened; today we are in what I call the nonpaperless society. We are producing more information on paper than we ever have throughout history, and we have millions of microcomputers with high speed printers that are producing paper at massive rates, tearing down forests at an unimaginable speed.

We're also using computers in such a way that we can automate our work, and that means we can talk more and we can communicate more information through talking than we ever have in the past.

Therefore, it is important that we identify the basic problem that we're dealing with and that we not create Maginot lines by creating a monolith of security around computers, when most of the information in those computers is on paper sitting on desks in unlocked offices. So we have an information security problem, not just a computer problem.

In my recommendations to clients in acquiring microcomputers with high-speed printers, I recommend that for every high-speed printer that's obtained they also obtain a shredder, and in fact, as

BEST COPY AVAILABLE

the paper is printed and comes out of the printer it automatically goes into the shredder except when you take something out to keep that from happening.

The point here is that the scope of this whole subject is simply too narrow, and we must consider information before it goes into the computer, and the massive amount of information coming out of computers on paper and through voice.

So in order to approach that problem properly, it seems to me that we need a baseline of security that applies generally-accepted controls and practices that we all know about across the whole range to protect information wherever it is in whatever form, and that we add to that special controls as necessary for special vulnerabilities, in order to avoid this Maginot line syndrome that I find so prolific throughout business and government.

We're making very rapid and significant advances in technological controls over information. The National Bureau of Standards, National Computer Security Center, Department of Energy, NSF, Department of Justice, and so on are advancing technological controls, but the problem we have that is rightly identified by 2889 is that here we are advancing in technological areas but we are not sufficiently advancing in human controls. That is, the discipline imposed on humans, which are obviously the weakest part of any system of information that we have.

We're also making very good progress in criminal laws with Congressmen Hughes and Nelson's bills, the administration bill from the Department of Justice, and the law that we now have in the title 18 code. So advances are being made there.

This bill, 2889, has the right thrust and the right subject; that is, dealing with the human controls on the human vulnerability side of information security. So I would recommend that wherever the term computer or telecommunications is used, that it be replaced with the term information so that it will concentrate on the assets subject to loss rather than just the mechanism for causing that loss.

Second, I address the education, awareness, and motivation issue addressed in the bill. Most people working in computer security today are computer technologists, and they think of solving problems technologically. Whereas, computers don't commit crimes or make errors; it's people that do that, and I think there has not been enough emphasis on the people side of the problem.

Security we find over and over again will not work unless there is a cooperation and an awareness of the need for it by people, and that is where 2889 is right on target.

Now, there's a problem here, however; security is a different subject than quality control or safety in work. Information workers see security as getting in the way of their job performance, it reduces their job performance on an individual short-term basis. It is counterproductive to the work that they do that results in their getting advances and salary increases.

Therefore, my point is that you can lead a "techie" to security training courses, but you can't make him think or accept it until there is a system of rewards and penalties associated with it. And therefore, I think that the direction of 2889 should be aimed toward the process of stimulating motivation through rewards and

BEST COPY AVAILABLE

penalties, which is the way that we know we can get cooperation and motivation from people to get them to do something that they otherwise don't see in their own self-interest.

And so we need to have training, we need to have awareness and motivation programs, but they will not work alone. And I know this from a lot of practical experience. Those programs will not work unless they are accompanied by a system of rewards and penalties. And in my testimony, I have indicated some examples of rewards and penalties and the need for that in education, awareness, and motivation.

No. 3, accountability. Security is first and foremost a line manager and information worker responsibility. Each individual has a responsibility, and each has to be held accountable for the information within their responsibility.

Security reduces productivity, as I said. And these information workers will beat us every time unless they understand that they are held accountable for the integrity and the security of the information within their area. Therefore, I recommend that a set of policies, codes of conduct that are signed at least once a year by every information worker, and performance and salary reviews be organized so that an information worker or a manager knows what he is accountable for, and he knows that he can gain advancement in his position by meeting the security responsibilities, and knows that he will be punished if he doesn't do that.

No. 4, the causes of loss. Among the 50 or so computer criminals I have interviewed, most of them engaged in their crime because of some intense, unshareable problem they were trying to solve. They perceive of themselves not as criminals but as problem solvers.

This has been borne out in studies done by the Federal Government as well.

One way in which we can address the basic cause of these kinds of information losses, therefore, is by helping people to share these intense problems and in solving them.

We find in the private sector and I think also in the Government sector as well, that an array of confidential advisory services to help people with intense problems associated with families, sex, financial, gambling, and drug abuse would have a major effect in reducing these basic causes of loss and in a very commendable way.

No. 5, you have addressed in 2889 the training of all people associated with computers. I suggest that be extended to all information workers, but there is a special need here.

I mentioned the technologists who are responsible for our computer security throughout Government agencies. These people are technologists. They have to be technologists because of the strong technical component associated with information security. These people are not security people. They have not been trained to be security people.

Within the Federal Government, the intelligence services, the military particularly, know what security is all about. Where security is in a person's job title, it means that person is in an army defending an organization from an enemy.

When I ask a computer security technologist what his job is, it is to implement safeguards such as password access controls, make sure there are strong electronic locks on doors, make sure there

BEST COPY AVAILABLE

are no vulnerabilities in computer operating systems. That is the wrong answer.

What I want when I ask a person who has security in his title what his job is, it is as I described, to protect an organization from an enemy and to do so in a variety of ways and not just through technological controls.

As I said, we are already well advanced in technological controls. The problem is using them correctly and understanding that it is a people problem before it is a technological problem.

Therefore, I recommend training, not only across the board for information workers, but particular training for information and computer security officers; in fact, cross training among security people and computer technology security people within the Federal Government.

Finally, No. 6 of my recommendations. I believe that there is a growing national array of vulnerabilities in the private sector and in the civil government sector, and that this must be addressed. This has been supported by several studies that have been done that I have identified in my written report.

The problem first of all is the recognition of what these vulnerabilities are. It is important that we have parallel research and enrichment of our current research. The idea of focusing security only in one or very few specific agencies, I think is not the correct approach.

I think that like research in the medical field, for example, we need independent parallel efforts, looking for the vulnerabilities and looking for the solutions, coming from different points of view.

I should say much of the security that we have in the civil government and in the private sector has come originally from the military. We continue to see a flow of technological safeguards and administrative safeguard ideas coming from the military environment. If you want to see what we will be doing in business and civil government in the next few years, look at what is going on in information security in the military today.

Therefore, we need a strong flow of that information. We need to assure that we are getting this kind of support from the military side.

We also need this approach to security from the civil side and from the private sector side, so that we get all prospectives looking at the information security problem.

I am not an expert on organizing Federal Government missions. I can't really comment specifically other than to say in my recommendation that we should be strengthening the National Bureau of Standards, also encouraging the National Computer Security Center, and other Government agencies that are all working on this same problem.

One last point. In the private sector, we also see a need for the same kind of thing I just described.

Lieutenant General Faurer 2 years ago, as head of the National Security Agency, called for a mechanism in the private sector, in the business sector, to parellel the efforts within the Government sector. A year or so ago SRI joined with AT&T American Transtech, to develop a new concept which we call the International Information Integrity Institute, that would develop a mechanism in

BEST COPY AVAILABLE

the private sector in some ways similar to the National Computer Security Center and NBS type of operation in the Government sector.

One of its functions would be as a conduit, a two way conduit, between the Government and the private sector, to assure adequate security from particularly national and international vulnerabilities.

There are three problems having to do with this, however, that we have to be concerned with, in the private sector particularly. We must not disturb in negative ways the economic balance: that is profitability, productivity, and market share in the private sector. Whatever is done in the Government sector in assisting the private sector in this area, this is an extremely important aspect.

The second point is national versus international. Our private sector is fundamentally international in nature, made up of foreign owned, partly foreign-owned companies, and multinational companies. Therefore, attempting to approach the problem from a nationalistic point of view in the private sector is a mismatch, and that is a problem that has to be dealt with. It is international in the private sector.

Third, we have to remember that while we get much of our security from the military environment, the civil government and the private sector areas' vulnerabilities, types of enemies we have to deal with and the environments in which we have to deal with them are in many respects different than in the military.

We have to deal with these three problems to assure that we have a prudent approach to security, both in the civil sector and the business sector.

We envision the development of the I4 operation as we refer to it, over the next year, starting it out as a pilot operation and expanding it throughout the private sector as far as we possibly can to provide this interface with what is going on in the Federal Government.

That ends my comments.

Mr. BROWN. Thank you very much, Mr. Parker.

Mr. Lewis, do you have any questions?

Mr. LEWIS. Thank you, Mr. Chairman.

You made a number of recommendations, Mr. Parker, regarding the nature of training to be provided. For example, advisory services for personal problems, et cetera. Are you suggesting that this be placed in the legislation in any way?

Mr. PARKER. I am not an expert on what must be done through legislation and what can be done in other ways. I will leave that to the experts.

I am simply pointing out that I see a very great need that is not being met by this particular legislation, having to do with those points that I made.

Mr. LEWIS. You also suggested rewards and penalties for good and bad performance. How would you suggest this be handled in the bill, if at all?

Mr. PARKER. I would think that some relatively general statements about implementing a system of rewards and penalties be stated in the bill, but that the particulars of carrying out that system be left to the individual Government agencies and to the

BEST COPY AVAILABLE

OPM or wherever that might properly fit within the administration.

Mr. LEWIS. Could you give us a little more explanation on I4 and how it would work and how this would be funded?

Mr. PARKER. I4 would be a privately funded, not-for-profit independent institute. It would provide an array of services to the private sector that would include an intelligence function of reporting vulnerabilities based on actual loss experience.

For example, we have a research file of computer abuse of over 1,700 reported cases since 1958. We learned a great amount from studying actual loss experience.

This information would be provided on a more organized basis through I4 to the private sector.

In addition, we are expanding a concept called the baseline approach to computer security that I mentioned before. That is, making sure that you have the generally accepted controls and practices in place before you start dealing with the more subtle kinds of vulnerabilities. Therefore, I4 would promulgate the expansion, use, and identity of generally accepted controls and practices.

We know a great amount about vulnerabilities today. We know a great amount about the good controls for those vulnerabilities. The problem is implementing those controls.

I4 would promulgate the identification, the reporting, and the use of generally accepted controls and practices. Many of those controls and practices are documented and come from the National Bureau of Standards, National Computer Security Center, and other parts of the Federal Government. I want to make sure that flow of useful information continues.

Mr. LEWIS. Thank you, Mr. Parker. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Walgren.

Mr. WALGREN. In your exposure as a private citizen, can you make any estimate of the size of the present Bureau of Standards Program? The witness from the Bureau estimated they were spending something in the range of $1 million on, I gather, security research and development of standards related to security.

How big an effort does that get you? What does the $1 million do for you in that area? Does it get you 10 researchers and some support for them?

Mr. PARKER. I would agree with that on the order of 8 or 10 professional researchers. I would consider that a very small effort. I think if you look at the size and depth of the information security problem, a much larger effort than that is needed in that particular area. The size of the National Computer Security Center effort, as I understand it, is considerably larger than that. I think that more effort should be placed in this area of research, development, and training, considering the importance of it, especially with the increasing issues of national vulnerability before us.

Mr. LEWIS. I would gather that with that amount of money, you would really be very hardware-oriented, would you not? If you only have $1 million and given the kinds of requests that must come into the NBS from the whole Federal Government which must be related to a configuration of one computer bit of equipment, which may be relatively unique to that operation versus the different equipment that might be available to other parts of the Federal

BEST COPY AVAILABLE

Government or procured by the Federal Government, that you would be very hardware-focused awfully fast, and not on people and not on information handling, but rather sort of solution-oriented to problems that are raised by what are very finite bits of the Federal spectrum.

Mr. PARKER. It is my understanding that the National Bureau of Standards is expanding its areas of expertise and attention beyond strictly technical and into the areas of good management of information security. I would like to see that aspect of it expanded significantly to match the level of intensity and effort going into the technical side of information security.

Mr. WALGREN. One of the things that was striking me, and I don't know whether it is sound, Dr. Brotzman indicated that he felt that the Bureau of Standards' effort was totally complementary to the effort they were involved in, and that there really was very little overlap.

I guess I am wondering if there is no overlap because it is so infinitesimal, it does strike me that they are involved in the same areas, and that the NBS, to the degree that they are technically oriented on equipment, is very much in the same area that the National Security Agency is focused on, evaluating the hardware, the structure of the computer. I see them as being very much in the same area and yet the testimony is they really are not interfering with each other at all.

Would that be because the efforts are so small that there is no way one effort could interfere with the other?

Mr. PARKER. I don't know enough about this to be able to explicate the overlap or the unique differences between the two. I would comment that it is extremely important in security, because of the nature of security, that we have a significant amount of overlap and in fact in some aspects an adversarial relationship, where one organization is attempting to solve a problem in one way and another is attempting to solve it in another way, and may the best man win, in order to accomplish this.

What we are dealing with is an intelligent enemy. The idea is you have to outthink that intelligent enemy. There are lots of them out there. Therefore, we need different kinds of people with different kinds of approaches among the good guys to deal with that highly diverse range of enemies.

Therefore, I see the concept of any kind of redundancy as long as it is properly coordinated and we get the benefit out of that, that might lead to different solutions to the same problem as highly beneficial because of this nature of security.

You might compare it, for example, to cancer research, where we have many different independent activities going on, looking at it from different prospectives and taking different kinds of approaches. A very great effort of reporting and competition, avoids overlooking anything in our work in cancer research.

It is the same thing in security. We have to make sure that we are not overlooking it. It is the vulnerability that we have not discovered yet that will get us in the end. You need different approaches to assure that.

Mr. WALGREN. Mr. Chairman, if I might ask one other question.

BEST COPY AVAILABLE

Do you have any reservations about the military being—maybe it is not military—the security side of Government being the major if only, and maybe only, structural agent involved. Is there knowledge of these systems that would by definition spill over into the military or the security forces of the country, as such, that you would have reservations as a civilian, seeing built into their base?

Mr. PARKER. I think it would be dangerous to have any one segment, the military, the civil and the private sector, having some form of dominance on the subject, because these are all important functions.

I mentioned three areas of particular concern to the private sector. At least two of those have a concern to the civil sector as well.

As I said, we get a great flow of useful security from the military and we have to keep that open and make sure that we do get that, because it is of a very great significance to us.

But that also has to be tempered with a different kind of environment and a different kind of enemy. The military is looking at an enemy with unlimited resources. In the civil side and in the business sector, we are looking at an enemy of great diversity with limited resources, and we have to keep those perspectives in the way that we develop security.

But NTISSC and in particular, the advisory board that was recommended by Congressman Brooks in the revision, as important mechanisms that should be in place to assure that we get a balance of looking at these problems from these different perspectives and the solutions as well.

Mr. WALGREN. Thank you, Mr. Chairman.

Mr. BROWN. Thank you very much, Mr. Parker. I have no further questions. We appreciate your testimony.

[The prepared statement of Mr. Parker follows:]

BEST COPY AVAILABLE

Testimony of Donn B. Parker Before the U.S. House of Representatives, Subcommittees on Transportation, Aviation, and Materials, and Science, Research, and Technology, on H.R. 2889, The Computer Security Research and Training Act of 1985, on October 30, 1985

H.R. 2889, Computer Security Research and Training Act of 1985, promotes and supports security in exactly the right functional direction. While I don't feel expert or knowledgeable enough to comment on how it should be implemented among the various government agencies, I have recommendations for the subjects it addresses, its impact, and the security needs in the private sector.

While many of those who have testified on H.R. 2889 have indicated that it is superfluous, I find that an extension of its intent and function would make it important legislation to meet the government's needs for adequate information security that are not now being met. Specifically, solutions to two problems--lack of information security, and awareness and motivation for good security among trusted people using sensitive information and computers--can be advanced by extending H.R. 2889.

My recommendations are thus to:

1. Extend the scope of the bill to all information in all forms and media without regard to technical means for creation, processing, communication, or storage.

2. Extend the requirement for information security education, awareness, and motivation to all information workers along with application of appropriate awards and penalties.

3. Provide for development of descriptions of sensitive information, code of conduct, policies, and job performance reviews that hold government workers accountable as managers, users, or custodians for the security of sensitive information in their charge.

4. Specify that confidential employee advisory services for personal problems be made available to trusted information workers.

BEST COPY AVAILABLE

5. Establish the requirement for specialized education of computer security officers and plant or building security officers, the former in security and intelligence skills as well as technical skills and the latter in technical skills by a process of cross-training.

6. Stress the need for multiple, parallel, and independent information security research in several government agencies to be more assured of comprehensive identification of vulnerabilities and solutions.

Discussing these suggestions in order--first, H.R. 2889 falls short in recognizing that the security of information, not just computers, is the more fundamental need. We are creating Maginot Lines when we concentrate our efforts on only technological protection of information in computers and communications. Predictions of the paperless society have not materialized. We have a non-paperless society today and are producing more sensitive information on paper than ever before with the use of millions of microcomputers, most having a high-speed printer attached. In addition, we are conveying more sensitive information orally than ever before, as computers are used to automate our work thus giving us more time to talk.

Thus, our problem today is information security, not just computer security, and in the future the need will probably be knowledge security as we start using expert computer systems with knowledge bases. After people, information and knowledge are the most important assets of business and government and must be protected in whatever form.

Second, the principal deficiency in computer security today is a lack of awareness of the need and motivation for good security among trusted employees. This deficiency is addressed in H.R. 2889 by Congressmen Glickman, Fuqua, Brooks, Brown, Wirth, Walgren, Nelson, Wyden, Hughes, Lewis, and Horton. My second, third, fourth, and fifth recommendations address this problem. I have found, in performing over 70 computer security reviews in the private sector over the past 16 years, that security is not effective until trusted employees are constrained by safeguards which they are willing to tolerate and support, since many such safeguards require extra effort beyond direct job productivity.

However, training and motivational efforts called for in the bill will not be effective unless there are accompanying rewards and penalties for recognized good and bad practices. A computer programmer can be sent to classes and made to read material, but he or she won't listen or respond unless self-interest exists. H.R. 2889 falls short in this regard.

BEST COPY AVAILABLE

Rewards for good security practices can include more favorable job performance and salary review evaluations, priority in office facilities and computer equipment usage, favored parking spaces, plaques, award ceremonies, and management recognition. Penalties can include adverse personnel file entries, reporting of poor practices to fellow workers, forced secret password changes, loss of privileges, and, in extreme cases, termination.

In businesses, I emphasize the need to confront information workers with clear and simple rules in policies, codes of conduct, and salary and performance reviews regarding authorized and unauthorized acts in automated workplaces. In such environments, the ethical standards of such acts may not be directly carried over from non-automated environments or from the informal computer environments of the past. Examples include personal use of computer time, copying and use of proprietary computer programs, and reading or harming others' computer data files. This confrontation is even more important with the explicit identification of authorized and unauthorized acts in new computer crime statutes.

I have interviewed over 50 so-called computer criminals and found that most of them had intense, unsharable problems that motivated their criminal acts. They saw themselves as problem solvers, not criminals. This finding has also been supported by much research in white collar crime. One conclusion from this is that information crime can be deterred to some extent by offering confidential help to trusted information workers with financial, alcohol, drug, gambling, social, workplace, and family problems.

An extremely important requirement for good information security is acquisition and use of intelligence concerning trusted employee aberrant behavior and activities. Most computer security officers and line managers whom I know are untrained in and unaware of this powerful security practice. Yet it is well known and practiced in many other security functions.

Computer security officers usually have computer technology backgrounds and don't understand the security profession. My own research for the Department of Justice and other recent studies indicate that the greatest threats to information and computers are from disgruntled trusted employees and employees with personal problems. Making line managers and technical security staff sensitive to detection of these problems on an informal basis and cultivating informal and formal informant networks are basic aspects of good security. Government intelligence services are expert in these security practices. They should provide this type of training to technical managers and computer security officers throughout government agencies where sensitive information is created, processed, stored, and communicated.

BEST COPY AVAILABLE

Training must include specialized courses for computer security officers in information and computer security subjects. The results will be more competent, cross-trained security staffs in both areas.

My sixth suggestion, for parallel research efforts, is supported as follows. At present, significant advances are being made in criminal law especially with legislation proposed by Congressman Bill Nelson and William J. Hughes, the Administration bill from the Department of Justice, and the current statute, Title 18, Chapter 47, Article 1030 of the U.S. Criminal Code. The best features of each combine well to meet the current needs.

Significant advances are also being made in technical computer safeguards as a result of the efforts of the National Bureau of Standards Institute of Computer Science and Technology and the new National Computer Security Center.

The evaluation of risks in government use of computers using comprehensive quantified risk assessment methods has been a failure and waste of valuable security staff resources. In-depth risk assessment should be reserved for the few specific critical vulnerabilities where adequate data on frequency and monetary loss are derivable. Most known vulnerabilities can be reduced by a more practical baseline approach using generally accepted and well-known safeguards and security practices. Many of these safeguards and practices and new methods for their evaluation and selection are being published by the National Computer Security Center, National Bureau of Standards, the Department of Energy, SRI International, and others.

Much of the security applied in the private, business, and non-military government sectors was first developed and used in the military and intelligence sectors. The use of identification badges, cryptography, and Tempest-conditioned equipment are examples. This transfer of security safeguards technology must be continued, and the National Computer Security Center and National Bureau of Standards are important mechanisms for that.

The private sector is becoming so dependent on concentrated, fragile, yet powerful information technology that national vulnerabilities are growing, as indicated in several impartial studies.* This situation justifies the national defense concerns identified in NSDD 145 and the expanded role of the Department of Defense. However, serious negative consequences must be avoided that could do more harm than good.

---

*Observations on the Resiliency of the U.S. Information Society. Rein Turn, et al. American Federation of Information Processing Societies, Arlington, Virgina. November, 1982.

BEST COPY AVAILABLE

Three issues are worthy of note in this regard. First, the profitability, productivity, and market shares must not be disturbed in harmful ways. Second, the private sector is international in its fundamental make-up. Foreign-owned and partly foreign-owned and multinational companies of national defense importance preclude an exclusive nationalistic approach. Third, it must be recognized that the vulnerabilities, enemies, and environments in the military are quite different in some respects from those in the non-military.

One potential solution is a mechanism that could be developed in the private sector that was called for two years ago by the then head of the National Security Agency, Lt. Gen. Lincoln Faurer. In response, AT&T American Transtech joined with SRI International to begin development of the International Information Integrity Institute (a detailed description has been submitted to the subcommittee staff). I4, as it is called, would provide a conduit for information between the private sector and several pertinent government agencies, including the National Computer Security Center and National Bureau of Standards. It would promote good security practices in business and offer computer-related loss information on a timely basis. I hope to see I4 developed next year.

BEST COPY AVAILABLE

Mr. BROWN. Our next witness is Mr. William Franklin, Associate Director of the Information Management and Technology Division of the General Accounting Office.

Mr. Franklin, we're glad to have you here again, and your full statement will appear in the record. You may proceed in any way that you wish.

STATEMENT OF WILLIAM FRANKLIN, ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY DR. HAROLD J. PODELL, GROUP DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GAO, AND RAYMOND J. WYRSCH, SENIOR ATTORNEY, OFFICE OF THE GENERAL COUNSEL, GAO

Mr. FRANKLIN. Thank you, Mr. Chairman and members of the subcommittee. We are pleased to be here today to provide our views on H.R. 2889 entitled "The Computer Security Research and Training Act of 1985." I have with me on my left Dr. Harold Podell, group director from our Information Management and Technology Division, and Mr. Ray Wyrsch, senior attorney from our Office of the General Counsel.

We have long been interested in ensuring the security of automated information systems, and during the past decade have issued over 40 reports related to information systems security. As stated in the bill, information stored in government computers and transmitted over connecting networks is vulnerable to unauthorized access and disclosure, fraudulent manipulation and disruption. Studies of computer-related fraud and abuse in Federal agencies show a costly and widespread problem of significant proportions.

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program in the Federal Government and the requirement that each Federal agency provide mandatory periodic training in computer security.

In this regard, we pointed out in our testimony yesterday that only 2 of 25 systems in the agencies surveyed have a formal security training program. There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage, processing and transmission.

We further believe that the bill can be effectively used as a vehicle for addressing other related computer security management, research and training issues as identified in previous GAO reports and testimony, and in the April 1984 report of the Subcommittee on Transportation, Aviation and Materials.

In particular, the subcommittee report recommended that, "The administration establish a central focus to ensure that all facets of computer security are addressed."

As we stated in our testimony on this bill before the House Committee on Government Operations, we must have a clear understanding of the levels of security required for the range of information involved, and we must have clearly established lines of respon-

BEST COPY AVAILABLE

sibility and authority. Right now there is considerable confusion in both of these areas.

We pointed out to the subcommittee that until recently, the Department of Defense developed computer and telecommunications security standards primarily for national security information classified pursuant to Executive Order 12356. Unclassified information standards are provided by the National Bureau of Standards pursuant to the Brooks Act and provisions of Executive Order 11717.

The Office of Management and Budget and the General Services Administration also have major statutory responsibilities for computer and telecommunications policy and standards. OMB, pursuant to the Brooks Act, the Paperwork Reduction Act of 1980 and its general mandate for oversight of executive branch activities; while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No. 1.

In September 1984, the White House issued NSDD-145, which established a Systems Security Steering Group as the focal point for both military and civilian information systems security. Together with an interagency committee, executive agent and the national manager, the steering group is to establish and coordinate policies and review and approve budgets for computer and telecommunications security efforts throughout the Government.

This structure created by NSDD-145 partially fulfills the Federal leadership recommendation in the Subcommittee's April 1984 report. However, the directive does not cover information in national systems that is sensitive but is not considered critical to national security.

NSDD-145 does recognize that OMB, NBS, and GSA have major functions to carry out with regard to the security of information and automated systems, but the directive places ultimate control over the functions exercised by these agencies in the administrative structure it established.

Activities of the civilian agencies are all made subject to NSDD-145 approval mechanisms. Therefore, there is a potential for confusion regarding similar mechanisms established by legislation for NBS, OMB and, GSA.

The following provisions of H.R. 2889 overlap similar provisions of National Security Decision Directive 145. Section 3 of H.R. 2889 provides for NBS to (1) perform research and conduct studies to determine the nature and extent of computer security vulnerability in Federal agencies and their contractors; (2) devise administrative, management and technical procedures and practices designed to protect the information stored, processed and transmitted by Government computers; and (3) develop guidelines for use by Federal agencies in training their employees and the employees of their contractors and of other organizations whose computers interface with government computers in computer security awareness and good security practice.

NSDD-145 gives the Director, NSA, as National Manager, responsibilities to (1) conduct, approve or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information; (2) examine governmental communications systems and automated information systems and evaluate their vulnerability to

BEST COPY AVAILABLE

hostile interception and exploitation; (3) review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

These provisions would seem to provide for different agencies to perform similar functions. However, it is difficult to judge the precise extent of overlap that enactment of H.R. 2889 would engender since the full range of NSDD-145 and its overall applicability to civilian agencies is unclear.

While we support the need for a comprehensive computer security research and training program, as proposed by H.R. 2889, we would suggest that since computer security research and training programs are carried out by DOD for all Federal agencies, for both classified and much unclassified information, that a clear understanding of DOD's role versus the roles of OMB, GSA, and NBS be established in conjunction with consideration of H.R. 2889.

In conclusion, we support the intent of H.R. 2889. We believe deliberations over this bill provide a good opportunity for the Congress to consider establishing a central focus for computer security in the Federal Government, and at the same time preserve more of the traditional roles of the various executive agencies as provided for in existing legislation.

More importantly, the broad leadership role that NSDD-145 assigns, predominantly to DOD, raises basic questions concerning the extent to which the defense establishment should be involved in policy formulation and program administration within the Government's civilian agencies. There can be no question that there is unclassified information stored in government computers and transmitted through telecommunications systems, the unauthorized disclosure or disruption of which could affect our national security interests.[1] It does not follow that DOD must be responsible for deciding what should be done to protect this information. The assignment of that responsibility is an issue of long-range importance that should be thoroughly considered by the Congress.

That completes my prepared statement, Mr. Chairman. We would be pleased to answer any questions.

Mr. BROWN. Thank you, Mr. Franklin. Just as a comment, you have pointed to the need for Congress to establish policy with regard to the issue of who is responsible for computer security, and what we are doing here is replaying an act that has been played for a number of years about the overall responsibility for the procurement, management and so on.

Mr. Brooks has been a leader, and it is clear that what he is trying to do in the amendments to this Act are a parallel to the process that he set up under the Brooks Act for procurement and management. It's supposed to be Governmentwide, the role set forth in the Brooks Act with regard to computer procurement and management, but it excludes those parts of the DOD that relate to strictly defense and security matters, and leaves them a great deal of discretion.

What we have today is a situation where the Defense Department is, in effect, moving in the computer security area to preempt

[1] Mr. Franklin meant to say ". . . our national interests . . ." instead of ". . . our national security interest . . ."

BEST COPY AVAILABLE

a large part of the role of the civilian agencies for the management of computer security.

I don't know that there is much to be gained from re-fighting this battle all the time. I think what we are interested in is effective results. But sometimes it is hard to get effective results without having a clear sense of direction which seems to be lacking in this area.

With that philosophical comment, I will call upon Mr. Lewis for any questions he may have.

Mr. LEWIS. Thank you, Mr. Chairman. Mr. Franklin, do you have any evidence that the NSA training programs are inappropriate for the civil sector? And have these agencies expressed dissatisfaction?

Mr. FRANKLIN. No. We are unaware of any agency's dissatisfaction.

Regarding the appropriateness, we have not done a study of that in particular. The points I made yesterday will give some insight into that. I described four elements that are necessary for an effective computer security program—management and then the safeguards. The safeguards are broken down into three components; technical, physical, administrative.

Now, a major program that should be in place is risk management. So what that means is that there are many components to that, such as identification of threats, vulnerabilities and risks. In my experience—and we haven't done a study, but we've done a fairly good job along those lines; the down side is that in using the trusted computer systems evaluation criteria, which we did use in our survey, that does have a hole right now. And what that hole is, is each of the categories—for example, labeling a system as B1, C1, B2, A1—those have not been costed out. They cannot tell us how much each of those costs. If you say that a collection of information is sensitive to the degree that you must procure a system that has features to the C1 level, or B1 level, we don't know what that costs. Neither do they.

Another down side is the risk management approach. In performing a risk assessment, you would think that it would be emphasized to compute, or attempt to compute, your expected loss in monetary terms. Economic terms. That's not being emphasized.

What is being emphasized is determine what your threats, vulnerabilities and risks are, and then postulate subjectively, with a fair amount of knowledge, what you think the counter-measures are that you need to put in place to offset that. And you cost those out, and hopefully choose your least-cost alternative.

Well, that's only half of the problem. You don't know whether what you've just costed out is appropriate because you didn't know the costs associated with your expected loss in the first place.

So those are two major holes. I'm sure they're working on them, but to our knowledge, they haven't been resolved yet.

Mr. LEWIS. How about problems with the cooperative NBS-NSA effort? How could NBS and NSA's activities best be coordinated to ensure that they complement one another and we do not have duplication?

Mr. FRANKLIN. I can't give you a precise answer on that. I wish I could.

BEST COPY AVAILABLE

Mr. LEWIS. Well, as good as you can get.

Mr. FRANKLIN. Well, we haven't gone into an in-depth study on that. There are many alternatives. The alternative presented in the bill is one feasible alternative; there are other feasible alternatives. And in the past, in some cases formally and in some cases on an ad hoc basis, they have worked very well together.

For example, there is a standard in place right now put out by NBS, a data encription standard, that I know first hand that NBS and NSA worked very closely on. And it was put out and I would call it a joint cooperative effort. That goes on a lot.

Now, there probably is a need to formalize that, and I can't sit here and give you a precise prescription or solution, but I cannot find any fault with the alternative expressed in the bill.

Mr. LEWIS. One concern that has been expressed repeatedly is that no one is in charge, and we need a focus for computer security issues. Can you address this concern with respect to H.R. 2889 as amended, and who will be in charge?

Mr. FRANKLIN. Let me give you a general answer and then I'll turn it over to Dr. Podell who actually held the interviews.

So far, in terms of issuance of generalized policy to be interpreted by agency heads, OMB has issued A-71, Transmittal Memorandum No. 1. Not a perfect document, but it was issued. Agencies have responded to that document in varying degrees.

Now, the down side is that we can find no evidence of OMB acting as truly a catalyst in the interpretation and implementation of what is in Transmittal Memorandum No. 1. Put it out there; agencies are expected to do it, and it looks like they just sat back and have taken a "wait and see" attitude.

Mr. FRANKLIN. I will turn it over to Dr. Podell.

Dr. PODELL. We met with officials from OMB. We asked them for copies of their written comments on the draft of NSDD-145 before it was signed. They stated that these comments were for the purpose of advising the President and could not be provided to GAO. We don't really know what actually occurred before NSDD-145 was signed.

We also had interviews with some of the Department of Defense officials, who were instrumental in developing NSDD-145. The impression we had, as we presented in our testimony on June 27 before the Subcommittee on Transportation, Aviation and Materials, is that the directive itself was signed without full concurrence and possibly some uncertainty by OMB.

That is a situation that we determined from the interviews, that there was no clear concensus or agreement on what the central focus should be. Perhaps that will help in response to your search for what is the central focus.

Mr. LEWIS. Thank you, Mr. Franklin and Dr. Podell. Thank you, Mr. Chairman.

Mr. BROWN. Mr. Walgren.

Mr. WALGREN. Am I hearing you right when you say that the first and foremost question is the value of what it is you are protecting from being lost?

Mr. FRANKLIN. That is right.

Mr. WALGREN. Would it seem that information would come in several different forms. One, in which we have a monetary interest

BEST COPY AVAILABLE

that it get misdirected, and I gather, for example, that we would not care whether we misdirected one Social Security check out of 100 million, and to fix that might cost you the whole value of the 100 million, so you want to make a very careful estimate of the loss that you could anticipate.

Mr. FRANKLIN. In some cases, I see a tendency to separate security, information security, computer security, telecommunications security, what have you, from other types of activities that go on in the ADP area.

Security, first of all, should be built in, in the design of a system. A lot of the problems that are being uncovered result from systems being put up without going through all the steps that should have gone through in order to design and develop that system in the first place.

You heard some testimony from other people—we have not done research yet—but you heard from HHS about certain systems there. As they go through a redesign or as they go through a system modernization effort, if the sensitivity is there and if the management commitment and awareness are there, and people have been trained and indoctrinated on what they need to be concerned about, security will be built in as they redesign the system.

Design and development need to be emphasized. It is much more costly to try to retrofit something. You don't know whether you are retrofitting it properly if your systems were put up in a halfway manner and then on top of that, you don't have the systems and procedures people mentioned by one of the witnesses, who can describe all of the inputs, processes, and outputs associated with that process. When he was saying "system," I think he really meant "process." It is from the time of generation of the information, data, transforming the information, some of it goes along a manual route, some of it hits transmission lines, some of it hits the actual computer system itself, all through that whole process——

Mr. WALGREN. Even anticipatory fixes cost something. Even if you are evaluating the system, you have to spend the manpower time to evaluate the system.

My question is, isn't the first step evaluating the degree of security that you want, and are there instances where you would say, well, we could design a system that would be highly secure but our anticipated losses do not match the expense to design that system, and therefore we should not bother to design the system.

Mr. FRANKLIN. Let me address the first part first. In evaluating a system, you must understand how it works. You cannot understand how it works unless you have documentation showing all of your information paths through that process, including the automated information system and telecommunications system.

In a lot of cases, that is the missing link. You do not know what all the paths are. You can't precisely identify all your vulnerabilities. The empirical data that you need to really do a comprehensive assessment of what your expected loss is, is not there. You really are taking a best shot, a guess, at what your expected loss is. You really have not built an accounting system to capture security information.

Let me refer to something GAO recommended a while back that related to all standards but security included. On April 19, 1978,

55-930 O - 86 - 7

BEST COPY AVAILABLE

GAO did a report on a Federal information processing standards program. One of the key recommendations had an item in it—let me read that to you—and it is referring to OMB.

He should establish a budget and cost reporting system that gives information on its efforts in the program and submit to GAO for approval an updated design of an accounting system which identifies funds spent on these efforts.

To my knowledge, that has not been done. I know it has not been done in the security area.

Mr. WALGREN. I guess I was wondering whether one of the factors in the dominance of a security agency approach or involvement versus a more civilian-dominated approach would be that instinctively the security agency requires security to be absolute. If it is classified, you do not want there to be one slip, and yet that is not the character of much of the information that we are apparently dealing with.

For example, if the downside is a very small misdirection of Social Security checks, it may be that our contention would not be constructively focused on that.

I guess what I am asking, when you say this issue raises basic questions of the role of the military and the like, is one of the downsides that a military or security bias to the system would be it would never ask the question of the cost of fixing the system to a very, very high degree of security? Is that a major downside of having the NSA substantially driving in this area?

Mr. FRANKLIN. It is difficult to answer in terms of saying they would never. What we can say is that in the past, with our being concerned with basically classified information, it becomes a secondary determinate. By that, what I mean is the objective is to counter the threat, whatever it takes.

Once you postulate alternative solutions to countering that threat, you pick the least cost alternative. The objective is to counter the threat. If you do not do that, then you really have not achieved what the mission calls for.

Mr. WALGREN. One of the nice things of having a military involvement here is that generally our society has given whatever it takes. The assessment was that the review of NSA's involvement in this by congressional committees never even raised the subject of limitation and therefore they assumed that was tacit approval of whatever they wanted to give to it.

Yet you get this program in a civilian area and we will limit that budget seven ways to Sunday, and limit it so much that not very much will happen.

Thank you, Mr. Chairman. I apologize for the ruminations.

Mr. BROWN. Mr. Glickman.

Mr. GLICKMAN. Thank you, Mr. Chairman. I apologize for being late.

I would like to follow on a little bit with what Mr. Walgren said. One of the statements yesterday from the very zealous Mr. Kusserow, the inspector general of the Health and Human Services, indicated that the National Security Agency basically had no interest in what HHS, the largest operator of civilian computers in our Government, had to say with respect to computer security.

BEST COPY AVAILABLE

I gather that one of the problems in giving the military the lead in this area is frankly their inclination is not to care about the implication of computer security problems in the civilian sector, the ones that actually affect most American lives.

I wonder how you would respond to that?

Mr. FRANKLIN. We don't have any evidence to show that they do not care. Really I don't believe that is the case anyway. I think what they were trying to do is stay within what they perceive as their charter. Throughout the NSDD document, what you will see is reference continually to national security related information. They have to stay within their national security realm.

What that means is if you have information that is sensitive for other reasons, it is sensitive in a national sense, not a national security sense.

They probably don't see themselves as having any authority to take a lead role over that. They probably have a lot of good information that they could share, but I think the cooperative effort between NBS and NSA is certainly needed. I agree with our last witness in that when you are dealing with an area whereby there are a lot of unknowns, this is one, and you do need a lot of coordination but you do need some amount of competition, too. That occurs in the procurement area all the time with fly-offs, where you attempt to get a solution to the same problem that nobody really knows how to solve, and you may get different approaches and hopefully one of those approaches proves out.

As long as those efforts are coordinated, there is really nothing wrong with that. That is the way it is done all the time in the research area. I am a researcher myself.

Mr. GLICKMAN. You testified yesterday and you provided a GAO report that spelled out in great detail the gravity of this problem. You referred to it again today in your testimony, how few Federal agencies have focused on this issue in a variety of ways. The committee has been provided detailed information with respect to each one of those systems.

In your testimony on pages 6 and 7, I am characterizing your testimony, you basically say that you support the intent of this bill, however, you have a couple of concerns which you would hope could be addressed. One is the overlap between the application of the NSDD-145 to the civilian agencies and the relationship between NSA and the Bureau of Standards, and I assume by that you are saying there ought to be a clear statement of the respective roles in the legislation.

Mr. FRANKLIN. Right. One thing that happens right now in the current environment of this bill is there is a category of information labeled as sensitive, unclassified but in the national security interest, that is the identification of a category that has yet to be defined. I don't think anyone can tell me what is in it and what is not in it.

One thing the bill does attempt to do is to create a boundary. The defense side, you have national security information and NBS, you have basically unclassified information. When you think about it, it basically follows along the lines of systems subject to the Brooks Act and systems excluded from the Brooks Act. It is not ex-

BEST COPY AVAILABLE

actly that clean but it is much better than the identification of a category with absolutely no definition at all.

Mr. GLICKMAN. Do you have any specific suggestions for further delineation of that bifurcation of authority?

Mr. FRANKLIN. Without an actual study, I cannot sit here now and prescribe a solution. At this time, there are issues relative to what situations are there, whereby systems that handle information that may be classified and unclassified, the equipment that those information systems are processed on is commercially available, general purpose, ADP equipment, giving the impression that it should probably fall under the Brooks Act, but yet critical to a defense mission in a way that falls maybe under one of the exclusion categories of the Warner amendment.

There is some issue there but that is not nearly to the degree of the problem that you have with a category called unclassified, sensitive, in the national security interest, when you do not have a definition of that category. No one can tell you what system, what information systems fall where.

At least with the Brooks Act and Warner separation, there are systems that are clear. You can clearly say that the retirement survivor's disability insurance system is not a Warner amendment system. That clearly falls over here. It clearly points out some defense systems that clearly fall on one side or the other.

There is a set of systems that still have to be discussed and debated. That is a lot different——

Mr. GLICKMAN. Like what? Give me some examples of those systems you just mentioned.

Mr. FRANKLIN. I know the acronym. I just don't know what all the terms in it mean. There is a system called DAS-3B in the military. That system is general purpose, commercially available ADP equipment, but because of the potential for going into the field, could legitimately fall under one of the exclusions. It has to be debated. I can't sit here and give you the answer.

There are a lot of systems like that, most of which are in the Defense Department. On the civil side, I can't think of an example that would fall in that situation.

Mr. GLICKMAN. Thank you very much.

Mr. BROWN. Mr. Lewis, do you have another question?

Mr. LEWIS. Yes. Mr. Franklin and Dr. Podell, I am not sure you answered my last question. I think you gave me a lot of mumbo jumbo about the OMB.

As you review 2889 as amended, who do you think is going to be in charge? This has been a concern that we have heard repeatedly over the past 2 days. Who do you think is going to be in charge of H.R. 2889 as amended?

Mr. FRANKLIN. It depends on what lines you are talking about. Let me give you a general answer and then I will turn it over to our attorney who can cite some things for you.

In general, as a practical matter, I think by having control of the purse OMB, by definition is in charge, but they are also given that authority under the Paperwork Reduction Act. If you are talking about who is in charge in terms of the authority to issue standards, clearly the act points out that NBS has sole responsibility.

BEST COPY AVAILABLE

When you think about it, they still have to coordinate the proposed standards with all of the agencies, including OMB. If they have to do that, OMB is going to look at it from the standpoint of how much is this standard going to cost us. I don't know whether they would look at it from the other side of how much is it costing us now without this standard. People don't look at it that way. They look at it as a new cost and they don't look at the offsetting costs of having the standard. The Government for the most part does not make these products, you buy them. To the extent that you require a standard, you may through competitive forces bring down the cost. If you don't, it will hit you on the back end because now you have to convert every time you do a competitive procurement. You go through a major conversion, that not only has a direct cost associated with the system, but an indirect cost because it ripples throughout the organization in some cases.

Mr. WYRSCH. In answer to your question, it would depend upon the function that is being performed. In the area of standard setting, there would be a more clearly defined role given to NBS, and in the area of procurement, there would be a clearly defined role with respect to GSA.

Ultimately, the person who would be in charge would be the Director of OMB. In terms of exercising his general oversight role and what have you.

But this bill would be, in our judgement, an improvement over the existing legislation in the sense that it would add more specificity to the role of NBS and GSA as well.

Mr. LEWIS. Thank you, Mr. Chairman.

I would hope so, but I am afraid we would be back here next year, trying to make the same determination.

Mr. BROWN. All right. If there are no further questions, gentlemen, thank you very much for your testimony. You have helped move us along in understanding this problem.

[The prepared statement of Mr. Franklin follows:]

BEST COPY AVAILABLE

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 AM, EST
WEDNESDAY, OCTOBER 30, 1985

STATEMENT OF

WILLIAM S. FRANKLIN

ASSOCIATE DIRECTOR

INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

AND THE

SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

H.R. 2889

BEST COPY AVAILABLE

Mr. Chairman and Members of the Subcommittees:

We are pleased to be here today to provide our views on H.R. 2889 entitled the "Computer Security Research and Training Act of 1985." I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of the General Counsel.

We have long been interested in ensuring the security of automated information systems, and, during the past decade, have issued over 40 reports related to information systems security. As stated in the bill, information stored in government computers and transmitted over connecting networks is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption. Studies of computer-related fraud and abuse in government agencies show a costly and widespread problem of significant proportions.

In developing this statement, we drew upon our June 27, 1985, testimony before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on the potential impact of National Security Decision Directive (NSDD) 145[1] on civil agencies[2] and our September 18, 1985, testimony before the House Committee on Government Operations which provided our views

[1]NSDD 145, National Policy on Telecommunications and Automated Information Systems Security, dated Sept. 17, 1984.

[2]Statement of Warren G. Reed, Director, Information Management and Technology Division, U.S. General Accounting Office, before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on the Potential Impact of National Security Decision Directive (NSDD) 145 on Civil Agencies.

BEST COPY AVAILABLE

on H.R. 2889.[3] Also, we drew upon our testimony given yesterday before the Subcommittee on Transportation, Aviation and Materials, on the status of computer security of selected information systems in civil agencies.[4]

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program in the federal government and the requirement that each federal agency provide mandatory periodic training in computer security. In this regard we pointed out in our testimony yesterday that only 2 of 25 systems in the agencies surveyed have a formal security training program. There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage, processing, and transmission. We further believe that the bill can be effectively used as a vehicle for addressing other related computer security management, research, and training issues, as identified in previous GAO reports and testimony, and in the April 1984

---

[3]Statement of Milton J. Socolar, Special Assistant to the Comptroller General, U.S. General Accounting Office, before the Subcommittee on Legislation and National Security, House Committee on Government Operations, on Computer Security Research and Training Act of 1985, H.R. 2889, dated Sept. 18, 1985.

[4]Statement of William S. Franklin, Associate Director, Information Management and Technology Division, U. S. General Accounting Office, before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on Automated Information Systems Security in Federal Civil Agencies, dated Oct. 29, 1985.

BEST COPY AVAILABLE

report of the Subcommittee on Transportation, Aviation and Materials.[5] In particular, the Subcommittee report recommended that "...the Administration...establish a central focus...to ensure that all facets of computer security are addressed...." As we stated in our testimony on this bill before the House Committee on Government Operations, we must have a clear understanding of the levels of security required for the range of information involved, and we must have clearly established lines of responsibility and authority. Right now there is considerable confusion in both of these areas.

We pointed out to the Committee that until recently the Department of Defense (DOD) developed computer and telecommunications security standards primarily for national security information classified pursuant to Executive Order 12356. Unclassified information standards are provided by the National Bureau of Standards (NBS) pursuant to the Brooks Act and provisions of Executive Order 11717. The Office of Management and Budget (OMB) and the General Services Administration (GSA) also have major statutory responsibilities for computer and telecommunications policy and standards--OMB pursuant to the Brooks Act, the Paperwork Reduction Act of 1980, and its general mandate for oversight of executive

---

[5] Computer and Communications Security and Privacy (Report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, dated Apr. 1984.)

BEST COPY AVAILABLE

branch activities, while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No. 1.[6]

In September 1984, the White House issued NSDD 145, which establishes a Systems Security Steering Group as the focal point for both military and civilian information systems security. Together with an interagency committee, Executive Agent, and the National Manager, the Steering Group is to establish and coordinate policies and review and approve budgets for computer and telecommunications security efforts throughout the government. This structure created by NSDD 145 partially fulfills the federal leadership recommendation in the Subcommittee's April 1984 report. However, the directive does not cover information in national systems that is sensitive but is not considered critical to national security.

The directive provides for safeguarding from hostile exploitation systems that process and communicate sensitive information. And here the definition of sensitive information has been broadened to include any information affecting national security interests whether classified or unclassified. It puts DOD and the civilian lead agencies in the same arena for large segments of information. However, this occurs without a clearly established division of responsibilities, at least until the scope of the new definition of sensitive information is specified.

---

[6]"Security of Federal Automated Information Systems," issued July 27, 1978.

BEST COPY AVAILABLE

NSDD 145 does recognize that OMB, NBS, and GSA have major functions to carry out with regard to the security of information in automated systems, but the directive places ultimate control over the functions exercised by those agencies in the administrative structure it established. Activities of the civilian agencies are all made subject to NSDD 145 approval mechanisms. Therefore, there is a potential for confusion regarding similar mechanisms established by legislation for NBS, OMB, and GSA. The NSDD 145 mechanisms diffuse the recommendation for a central focus contained in the April 1984 Subcommittee report.

The following provisions of H.R. 2889 overlap similar provisions of National Security Decision Directive 145. Section 3 of H.R. 2889 provides for NBS to

--perform research and conduct studies to determine the nature and extent of computer security vulnerability in federal agencies and their contractors;

--devise administrative, management, and technical procedures and practices designed to protect the information stored, processed, and transmitted by government computers; and

--develop guidelines for use by federal agencies in training their employees, and the employees of their contractors and of other organizations whose computers interface with government computers. in computer security awareness and good security practice.

NSDD 145 gives the Director, National Security Agency, as National Manager, responsibilities to

BEST COPY AVAILABLE

--conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information;

--examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, executive orders and applicable presidential directives. No monitoring shall be performed without advising the heads of the agencies departments or services concerned; and

--review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

These provisions would seem to provide for different agencies to perform similar functions. However, it is difficult to judge the precise extent of overlap that enactment of H.R. 2889 would engender, since the full range of NSDD 145 and its overall applicability to civilian agencies is unclear.

While we support the need for a comprehensive computer security research and training program as proposed by H.R. 2889, we would suggest, that since computer security research and training programs are carried out by DOD for all federal agencies for both classified and much unclassified information, that a clear understanding of DOD's role versus the roles of OMB, GSA, and NBS be established in conjunction with consideration of H.R. 2889.

BEST COPY AVAILABLE

In conclusion, we support the intent of H.R. 2889. We believe deliberations over this bill provide a good opportunity for the Congress to consider establishing a central focus for computer security in the federal government, and at the same time preserve more of the traditional roles of the various executive agencies as provided for in existing legislation.

More importantly, the broad leadership role that NSDD 145 assigns predominantly to DOD raises basic questions concerning the extent to which the defense establishment should be involved in policy formulation and program administration within the government's civilian agencies. There can be no question that there is unclassified information stored in government computers and transmitted through telecommunications systems, the unauthorized disclosure or disruption of which could affect our national interests. It does not follow that DOD must be responsible for deciding what should be done to protect this information. The assignment of that responsibility is an issue of long-range importance that should be thoroughly considered by the Congress.

- - - - -

That completes my prepared statement, Mr. Chairman. We would be pleased to answer any questions.

BEST COPY AVAILABLE

Mr. BROWN. And our last witness this morning will be Mr. Terry Culler, Associate Director, Office of Personnel Management.

Mr. Culler, there have been a number of references to the important role that personnel training and improved management has in this overall problem, and you are going to tell us how you are going to handle that, aren't you?

STATEMENT OF TERRY W. CULLER, ASSOCIATE DIRECTOR, WORK FORCE EFFECTIVENESS AND DEVELOPMENT, OFFICE OF PERSONNEL MANAGEMENT

Mr. CULLER. Well, I will tell you what we are doing now to the best of my ability, and I will tell you what our position is on 2889 as it is now written.

Mr. BROWN. I can guess that.

Go ahead, though.

Mr. CULLER. Thank you, Mr. Chairman.

I am pleased to have the opportunity to testify here today on H.R. 2889, the Computer Security Research and Training Act of 1985.

We, at OPM, will defer to the Department of Commerce and to the other agencies of Government on the substantive aspects of computer security. Our testimony will be solely based on those provisions of 2889, which reflect on the Office of Personnel Management.

This act would assign to the OPM responsibility to issue regulations prescribing in detail the procedures and scope of computer security training to be provided by Federal agencies for their employees and for personnel of contractors who are involved with the management, use or operation of computers, which interface with Government computers.

The National Bureau of Standards would provide guidelines for use by Federal agencies in training their employees, and the employees of contractors and other organizations whose computers interface with Government computers, in computer security awareness and good security practice.

It is our view that the Office of Personnel Management has now adequate legislative authority to provide other Federal agencies with guidance on training related to computer security and further, may do so without the need to issue additional regulations as called for in the act.

The Government Employee Training Act, which is now codified in chapter 41 of 5 U.S.C., directs the OPM to prescribe regulations on Federal training and coordinating training activities of agencies in the Federal Government. And we have done so, and our regulations are found at 5 CFR 410.

The Office of Personnel Management also has authority to establish interagency training programs for Federal agency employees, in effect we provide training. We currently operate such a program in the area of information resources management.

We also have authority to assist Federal departments and agencies in their intraagency training programs, and we plan to continue to aggressively use these authorities to assure that training

BEST COPY AVAILABLE

needs associated with all aspects of computer security in the government, are met.

As I said before, we do not feel that the provisions of the bill which pertain to the Office of Personnel Management are necessary, and we are, therefore, opposed to the provisions of H.R. 2889.

I would like to make one further comment with regard to the development and delivery of training in the Government. OPM has launched a rather major effort in the last year to help agencies make greater use of the training resources that are found in academia and in the private sector, both to achieve greater economies in Federal training and to widen their scope of providers. And we believe that these resources can be effectively brought to bear in meeting computer security training needs of agencies, as well as in our own interagency training program.

I thank you for this opportunity to testify, and I will be happy to answer any questions.

Mr. BROWN. Thank you very much, Mr. Culler.

Mr. Culler, the GAO report on training and general computer security area has indicated that out of, I think, 25 agencies that they went into, only two of them, if I recall correctly, had what they would consider adequate training programs.

Would you care to comment as to whether or not that represents the realities of the situation. And if such is the case, whether or not this would indicate OPM is not giving a high enough priority to the training in this area.

Mr. CULLER. I can't really say whether their findings are capable of being spread across the entire Government or not. The Government Employees Training Act gives responsibility to the head of each individual agency, to determine what training will be given to the employees within that agency to better meet the needs of its mission.

We know that there are many, many training programs in information resource management going on in the Government today. To give you an example, among those that we operate, we conduct 59 different courses in the broad area of information resources management, and last year we ran about 1,200 sessions of those courses and trained somewhat in excess of 20,000 Federal employees.

Each of those courses has at least a segment in computer security in it. Two of the courses are dedicated solely to computer security.

The General Services Administration also offers interagency training programs in information resources management. We heard earlier today about some of the training programs of the National Security Agency. We know the Department of Defense offers training programs in the same area. So, while the programs may not be completely coherent throughout each and every agency in the Government, there are obviously large numbers of people who are receiving training.

I think we would be hesitant to see the Office of Personnel Management try to make decisions for the heads of individual agencies as to which individuals need to be trained when, in order to do their job better in any particular aspect of their job. It is something

BEST COPY AVAILABLE

that we have tried to avoid both in OPM and in its predecessor agency, the Civil Service Commission.

Mr. BROWN. Well, the problem is undoubtedly one of perception of the priority to be attached to this.

We have recently seen a great increase in the awareness of the importance of security in our national defense agencies. All these spy trials and whatnot have made us very much aware of it.

There hasn't been a similar broad perception of the losses that we might have from breaches of computer security, and hence it is not possible to say just how important that is. The focus of this legislation is aimed at increasing the priority on computer security.

One of the witnesses this morning indicated that there were probably several million people that ought to be involved in awareness, at least, of the importance of computer security. And that compares with how many, would you say, have actually be trained in computer security or computer-security awareness? A few thousand or something like that?

Mr. CULLER. That would be very difficult for me to say, sir. As I said, we ran about 20,000 people last year through our information resource management courses, and each of the courses has at least a segment on IRM.

As to how many have actually been through courses in other agencies or offered by academic institutions or private sector contractors, we have no way of knowing.

Mr. BROWN. Do you have any questions, Mr. Lewis?

Mr. LEWIS. One, Mr. Chairman. You asked my first question.

We have heard a lot this morning about commitment. Is there any way you can teach commitment? I know it is more an attitude, more than anything else.

Mr. CULLER. I don't know how to give you an answer to that, sir.

One of the gentlemen who testified earlier, talked about the use of performance appraisal systems—I don't think he used that phrase, but he used incentives and rewards—to encourage managers and other technical personnel to pay attention to security programs.

While I would personally be loathe to see a mandated element in everybody's performance standards throughout the Government, I think it would certainly be appropriate wherever an individual has responsibility for managing information, that their superior managers include elements in their performance standards having to do with computer or information security. That, in itself, I think would go to the commitment problem.

I am not at all convinced that running people through training courses is going to make them committed.

Mr. LEWIS. Thank you.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Mr. Culler, have you had a chance to look through the GAO report that was submitted to this committee yesterday, which outlined in my judgment the significant failure in most Federal agencies to deal with computer security in a very effective manner?

Mr. CULLER. No, sir, I have not seen that.

Mr. GLICKMAN. You really ought to read it, because given your job at OPM, you ought to see first hand how sorry the federal

BEST COPY AVAILABLE

system is in terms of implementing computer security as—if nothing else—as a consciousness factor in all stages of the operation of federal agencies.

Mr. CULLER. Yes, sir, I will make a point of reading that.

Mr. GLICKMAN. And also, you ought to read the testimony that GAO talks about, that this is not only an issue for their computer programmer, but it is an issue for the Secretary of the Department to be concerned about.

And you ought to look at the testimony of the inspector general at HHS, a self-described zealot on the issue, who is very, very clear in his feeling that his zealotry is not shared in very many other places in the Federal system. I would encourage you to look at that.

The other thing is, that if this bill is passed—even though you don't support it—if the bill is passed, what would be your role in implementing it? What would you do different than you do now?

Mr. CULLER. We would have to issue under this bill as it is now written, more regulations which, taking standards that would be developed by the National Bureau of Standards, would set forth to the Federal agencies, both what they should include in their training programs on computer security, and who should receive that training.

We are a little uncertain as to how we would actually define those who would receive the training. An earlier witness today talked about potentially 4.8 million people, I think was the number that was used, including contractor personnel.

That is an awful lot of people, and they all wouldn't need the same amount of training. They wouldn't need the same type of training. And we would have to look very carefully at that. I think it would not be an easy thing for us to define.

Mr. GLICKMAN. Well, that is a red herring, to say that 4.8 million people would need this kind of training. After all, you are supposed to provide the training now, aren't you?

I mean, people are supposed to be sensitized and trained in this area right now.

Mr. CULLER. We provide the training. "We," OPM, as a training provider, provide training to those agencies who come to us and say, "We want to have our people trained in this course, which you list in your course catalog that is published each year."

Or, they go to GSA, or they go to National Security Agency or whomever.

We provide the general rules for training. But, as I said, it has been our position historically, that it is the responsibility of the head of each department or agency to determine who needs what training in order to better fulfill their mission.

Mr. GLICKMAN. That would not necessarily be modified by this statute though, would it, if it were made?

I mean the agency, if it were still—I presume some discretion would be left in each agency to determine who would need training and who wouldn't.

Mr. CULLER. Yes, sir, that is true. Although the provisions of the bill as we read them, with regard to who should be receiving this training, would seem to require OPM in issuing regulations, to make some sort of delineations.

BEST COPY AVAILABLE

And to the degree that we would, in our regulations, be delineating classes of people, we would be restricting the parameters of the operation of the agency.

Mr. GLICKMAN. So you would perceive some clarification that would presumably give this role more directly to the agencies themselves?

Mr. CULLER. Yes, sir. If the bill were to pass.

Mr. GLICKMAN. Thank you, Mr Chairman.

Mr. BROWN. Thank you, Mr. Glickman.

I have no further questions, Mr. Culler.

Thank you very much for helping us out this morning.

The subcommittee members will stand adjourned.

[Whereupon, at 12:18 p.m., the hearing was adjourned.]

BEST COPY AVAILABLE

APPENDIX

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Honorable George E. Brown, Jr.
Chairman, Subcommittee on
Transportation, Aviation
and Materials
Committee on Science and Technology
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This is in response to your request of October 3, 1985 that I testify before your Subcommittee on October 29 concerning Federal computer and communications security and H.R. 2889, the "Computer Research and Training Act of 1985."

As Fred Upton of OMB discussed with your staff, I was unfortunately not able to attend the hearing. However, as promised I am enclosing a statement for the record. In addition, I would be pleased to provide answers to any questions you or the Subcommittee may have for the record.

Thank you for your interest in this important subject. If I can be of further help, let me know.

Sincerely,

Joseph R. Wright, Jr.
Deputy Director

Enclosure

BEST COPY AVAILABLE

FOR THE RECORD DRAFT
Release expected at 10:00 a.m.
Tuesday, October 29, 1985

STATEMENT OF JOSEPH R. WRIGHT
DEPUTY DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES
ON COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY
PROGRAMS IN THE FEDERAL GOVERNMENT
AND H.R. 2889 THE COMPUTER SECURITY RESEARCH
AND TRAINING ACT OF 1985

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to provide this Subcommittee our views on efforts to provide government-wide policy guidance and assistance on computer and communications security in the Federal Government and H. R. 2889, the "Computer Security Research and Training Act of 1985."

Historical OMB Interest in Federal Computer Security

As you may know, assuring adequate security of Federal automated information systems has been a concern of my Office for many years. Our interest in security has been heightened as the extent to which we as a society have accepted and used computers in all facets of our lives has grown dramatically, often without full recognition of their vulnerability. Sophisticated

BEST COPY AVAILABLE

technology that a few years ago was the sole province of the technocrat is increasingly being placed in the hands of any user. Soon a computer in the home could well be as widely accepted as a telephone. Very basic changes are taking place in the ways in which our society operates; the automation of information processes is at the heart of these changes.

Naturally, the Federal Government has participated in this revolution, since we are the Nation's largest user of automated information. Our investment in information technology is huge: We currently spend about 1.6% of our budget for ADP and telecommunications equipment and services, which in 1986 represents more than 15 billion dollars. The General Services Administration (GSA) estimates that we currently operate more than 17,000 medium and large scale computers. Moreover, as we integrate end-user computing into the management of Federal programs through the use of microcomputers, GSA estimates we could have as many as 500,000 micros in place by 1990.

The Department of Commerce's Federal Information Processing Standards program is an effort to confront the very serious problems of hardware and software compatibility that this exponential growth will bring. Communications standards will enable agencies to share and consolidate information when appropriate.

In the mid 1970's, Congressional concern over a number of issues helped focus our attention and stimulated our efforts in the computer security area. Hearings leading to the Privacy Act of 1974 pinpointed the potential for harm that automated data banks might represent to individuals. In other hearings, the Congress focused on the operational integrity of important automated systems such as the NORAD Air Defense System and the FAA Air Traffic Control System. In addition, a 1976 Congressional staff study focused directly on Federal computer security and system integrity issues.

BEST COPY AVAILABLE

OMB Circular No. A-71, Transmittal Memorandum No. 1

During the 1970's, computer security was perceived to be the sole responsibility of the computer facility rather than an overall management concern. To involve top management actively in this area, OMB used the authority for ADP policy given us by the Brooks Act (P.L. 89-306) and issued Transmittal Memorandum No. 1 to OMB Circular no. A-71, "Security of Federal Automated Information Systems". This Circular, issued in July, 1978, established a basic Federal computer security program. It requires that each agency head:

- Name a computer security officer for each computer installation;
- Establish personnel security policies which provide for screening of individuals involved in design or having access to sensitive computer processing systems or data;
- Establish a management control process to assure that appropriate levels of physical, technical and administrative safeguards are incorporated into data processing applications and facilities;
- Establish an agency program for periodic audits; and,
- Assign responsibility for the conduct of periodic risk analyses of each agency computer installation.

To broaden the base for oversight of this program OMB directed other central management agencies to provide assistance within their areas of expertise. Thus, Transmittal Memorandum No. 1 provided that the:

- Department of Commerce should develop and issue standards

BEST COPY AVAILABLE

and guidelines for ensuring the security of automated information.

- GSA should:
  -- issue regulations governing the physical security of computer rooms;
  -- assure that agency procurement requests for computers or related services adequately incorporate computer security considerations; and
  -- assure that procurement specifications for computer hardware, software, facilities or services are consistent with Commerce, OMB, and OPM standards.

- OPM should establish personnel security policies that provide for security consideration in the selection of personnel associated with design, operation or use of computer systems.

This effort represented the best available solution for the time. But, we should remember that it was a time when most computer centers were discrete entities, teleprocessing applications were limited, and agencies were not sharing much information. Our effort was aimed at putting management controls in place quickly and we believe it resulted in the creation of a computer security program that was effective for its time.

The Paperwork Reduction Act of 1980 reinforced the policy and approach established in Circular No. A-71, TM 1. Simply defining information as a valuable resource implies that it must be adequately secured when in automated information systems. Furthermore, that Act goes on to assign responsibility to the Office of Management and Budget for assuring the security of information in Federal automated information systems.

We recognize that times are changing dramatically. In the 1980's we have become substantially more dependent on automation for the

BEST COPY AVAILABLE

operation of many Federal programs. As Federal programs grow larger, automation provides the most effective and efficient means of administering those programs. Manual systems in many cases are simply not capable of providing an acceptable alternative, even in the limited role of a backup system. Can anyone imagine processing Social Security retirement checks by hand? Or managing a large inventory, such as the Defense Logistics Agency's two million stock items? Only in an automated environment could the Department meet its material management responsibilities with the speed and certainty national security requires. At the same time control over and access to those automated information resources is much more widely dispersed.

This rapid growth in our reliance on information technology brings the need for an effective Federal security program into sharp focus. We think that many of the elements of such a program are already in existence. OMB and the other central management agencies have produced a substantial body of material including directives, guidelines, and standards intended to assist agencies in dealing with the problem of information technology security. For example, the National Bureau of Standards has published numerous FIPS Publications concerning various aspects of security, including recent standards on password usage and computer data authentication.

In 1983, the President's Council on Integrity and Efficiency issued an initial report on Federal computer crime. The findings of that report cite "lack of knowledge" of systems controls as a particular point of vulnerability in Federal systems. In most cases an absence of adequate security would not be due to a lack of adequate tools, but rather a combination of lack of knowledge of those tools and lack of understanding by managers of the need to use such tools. Therefore, we have undertaken a two part approach to enhance Federal computer security by (1) clarifying responsibilities for security in revised policy guidance, and (2) raising security consciousness on the part of those who design,

BEST COPY AVAILABLE

maintain and use automated systems.

Revised Government-wide Policy Guidance

As part of a proposed consolidation and revision to four OMB Circulars, A-71, A-90, A-108, and A-121, our policy guidance on security of automated information systems is in the final stages of being revised. Our intent is to raise the awareness of Federal managers to the security risk in their automated information systems, clarify responsibilities for addressing that threat and provide a set of controls for use in reducing the security risk.

On March 15, 1985 a draft was published for comment. That proposal would put ultimate responsibility for the security of Federal automated information systems squarely on the shoulders of users of those systems. Unless users of Federal automated information systems want security as a feature of those systems, little security will be built in. In the past, users often tended to assume that security was a technical problem and not their concern. Under our revised policy guidance, that will no longer be the case.

The March 15 proposal also called for each agency to establish a security training and awareness program. Those programs are in part intended to raise the awareness of users of automated information systems to the vulnerabilities of their systems. Our objective is to stimulate user demand for security features in automated systems.

We are currently reviewing and incorporating public and agency comments and expect to issue the new Circular later this fall.

On August 16, 1983, we released OMB Circular No. A-123 implementing the Federal Manager's Financial Integrity Act (P.L. 97-255). It prescribes policies and standards for departments

BEST COPY AVAILABLE

and agencies in establishing, maintaining, evaluating , improving and reporting on internal controls in their program and administrative activities. Federal agencies have put forth substantial effort to evaluate the vulnerability of their programs and to take measures to reduce their vulnerability. An important part of those efforts has been an evaluation of the automated information systems that support those programs. The most often cited material weakness in internal controls reputed by agencies last year was in their ADP systems. As a follow-up, this year I asked agencies to include a summary of their accomplishments and plans for evaluating internal controls in automated systems in their annual report to the President and the Congress required by P.L. 97-255.

Relation of NSDD 145 and OMB Government-wide Policy

Your letter of invitation indicated your interest in the relation National Security Decision Directive No. 145 (NSDD-145), "National Policy for the Security of Telecommunication and Automated Information Systems" to OMB government-wide policy. NSDD-145 established Executive branch policy, created organizational structures and assigned responsibilities for assuring the security of National Security related information in computer and communications systems. It was issued because automation and communication of greater and greater amounts of national security-related information without special attention to the security of systems handling that information represents a growing threat to our national security.

As you know, under the Paperwork Reduction Act of 1980 my Office is responsible for assuring the security of information in Federal automated systems. There is specific authority to develop and implement policies, principles, standards and guidelines on safeguarding information collected or maintained by or on behalf of agencies, as well as authority to provide agencies with advice and guidance about information security.

BEST COPY AVAILABLE

The revision to Circular No. A-71, TM 1 in part implements that authority.

There are numerous instances, however, where types of information, such as tax information or census information, require special handling under separate authority due to the sensitivity of the information involved. In those cases, primary responsibility for assuring the security of that type of information is left to the agency primarily involved. The case of national security information is another instance where special procedures for handling information are authorized by separate authority. We believe that such authority is consistent with general OMB authorities concerning the security of all Federal information.

From an information policy perspective, NSDD-145 makes sense. OMB Circular No. A-71, TM 1 and proposed successor policies ultimately base the amount of protection to be afforded an information system on the risk and magnitude of loss or harm that would result if the security of the system were breached. The determination of potential harm is made by Federal agencies, and thus is based upon harm that the agency can best assess. In the case of national security information, however, there is a need to develop a common understanding of the magnitude of the threat, the implications of this threat to the protection of national security information, and the technologies applicable and appropriate to meeting this threat. To assure that adequate security is provided in those cases, it makes sense to maintain an organizational structure centrally that can identify weaknesses and require agencies to tighten up certain systems of concern to the national security.

I should add that we do not see a conflict between the NSDD and OMB directives concerning security of automated information. The OMB directives address the security of all information in Federal automated information systems and set minimum requirements on

BEST COPY AVAILABLE

agencies to secure their information. The NSDD applies only to national security-related information, and the mechanisms established under it will mandate additional protections for information that must be protected for reasons of national security. The OMB directives address security of automated information systems to include assuring that the systems do exactly what they are supposed to do, and nothing more. The NSDD is primarily concerned with protecting systems in such a way that national security information in them cannot be compromised.

OMB staff have actively participated in implementation of the NSDD, and we sit on each of the organizations established by it. Furthermore, in accordance with the NSDD, we have issued two OMB Bulletins calling for agencies to report information on the state of security of their systems that process classified national security information. Initial agency responses are tending to bear out the need for greater attention in this area. It indicates that existing security methodologies such as risk analyses and accreditations are not being employed at many Federal facilities.

Views of H. R. 2889

Your letter also indicated an interest in our views on H.R. 2889, the "Computer Research and Training Act of 1985." We believe that we already have a number of activities underway which are intended to address the same concerns which led to the introduction of H.R. 2889.

Section 3 of H.R. 2889 would establish a computer security research program at the National Bureau of Standards. We believe that the Bureau already has the requisite authority and has established such a program. That program is consistent with functions assigned to the Bureau by the Brooks Act, the Paperwork Reduction Act, and OMB Circular No. A-71 as well as the proposed revised circular. Furthermore, the Bureau has already issued

BEST COPY AVAILABLE

considerable guidance on securing automated information systems, to which I alluded earlier. Therefore, we see no need for new legislative authority in this area.

Section 4 of the bill would require training by all Federal agencies in computer security in accordance with regulations issued by the Office of Personnel Management. As I mentioned earlier, the proposed revision to OMB Circular No. A-71 includes a requirement for agencies to establish awareness and training programs in security of automated information systems. Here again, we believe adequate legislative authority exists, and we see no need for new authority.

We are also concerned about explicit authority that would be granted to OPM in the bill to issue detailed regulations prescribing the procedures and scope of agency training programs. We believe specific direct authority to OPM in this act is not consistent with OMB authority in the Paperwork Reduction Act. At a minimum, there is a high potential for agency confusion if OPM is given such regulatory authority. Furthermore, given the distinctly different activities different agencies are engaged in they need flexibility to design training programs that clearly meet with other agency activities. Detailed OPM regulations may seem counter to such flexibility.

Last week, the Subcommittee on Legislation and National Security of the Committee on Government operations substantially amended H.R. 2889 to become the "Computer Security Act of 1985." The revised bill would define more specific responsibilities and authorities for Federal computer security activities than the previous version. It also would create new oversight and disapproval authorities over agency information systems. We oppose this revised bill.

As we have outlined, the executive branch has a number of activities already underway that are aimed at tightening Federal

BEST COPY AVAILABLE

computer security. Passage of this bill would not contribute to those efforts and may actually impede them by adding confusion over responsibility for computer system security. Furthermore, this bill is not consistent with information resource management responsibilities established under the Paperwork Reduction Act of 1980. If it were enacted, it would require rethinking of responsibilities for information resources management in Federal agencies, and quite possibly legislative clarification of how those relate to computer and telecommunications security responsibilities in H.R. 2889.

Finally, the bill would base veto control over use of information technology on one facet of the technology--security. Arguments over adequacy of a security plan for sensitive systems could easily be quite lengthy--to the detriment of effective management and use of technology by agencies.

In closing, let me reiterate that our interest in the security of automated information systems is not a new one. It has been an area of concern to us for some time. Furthermore, we share the Subcommittee's concern that Federal automated information systems be properly protected. The sole purpose of Federal information technology is to effectively and efficiently carry out governmental functions. Assuring proper levels of security during the processing in such systems is essential to that purpose.

That being said, however, we believe that the original H.R. 2889 would not add to efforts the executive branch has underway to tighten security of Federal information systems, and the revision may even detract from these efforts. We would be pleased to answer any questions you may have for the record.

BEST COPY AVAILABLE